A SECTION WHITE PAPER:
A CALL FOR ACTION FOR ONLINE PIRACY AND COUNTERFEITING LEGISLATION

AMERICAN BAR ASSOCIATION
Section of Intellectual Property Law

A SECTION WHITE PAPER: A CALL FOR ACTION FOR ONLINE PIRACY AND COUNTERFEITING LEGISLATION

Section of Intellectual Property Law
AMERICAN BAR ASSOCIATION

Printed in the United States of America.

18 17 16 15 14 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

A call for action for online piracy and counterfeiting legislation : Section of Intellectual Property Law, American Bar Association.

pages cm
Includes bibliographical references and index.
ISBN 978-1-62722-823-7 (alk. paper)

1. Copyright—United States—Electronic information resources. 2. Copyright and electronic data processing—United States. 3. Piracy (Copyright)—United States—Prevention. 4. Copyright infringement—United States. 5. Product counterfeiting—United States—Prevention. 6. Counterfeits and counterfeiting—United States. 7. Computer crimes—United States. 8. Intellectual property—United States. I. American Bar Association. Section of Intellectual Property Law, issuing body, sponsoring body.
KF3024.E44C35 2014
346.7304'8—dc23 2014021166

Discounts are available for books ordered in bulk. Special consideration is given to state bars, CLE programs, and other barrelated organizations. Inquire at Book Publishing, ABA Publishing, American Bar Association, 321 N. Clark Street, Chicago, Illinois 60654-7598.

www.ShopABA.org

CONTENTS

INTRODUCTION: BALANCING THE INTERESTS

I. SECTION POSITION

The IPL Section supports legislation for effective copyright and trademark enforcement against Internet-based piracy based abroad, and that such legislation be adequate, effective, and efficient, but also addresses only the "bad" actors and with mechanisms that are fair and respectful of the due process rights of defendants and other innocent Internet businesses and users.

II. SECTION RESOLUTIONS

A. Resolution TF-02

RESOLVED, that the IPL Section supports, in principle, legislation to more effectively combat Internet-based copyright and trademark infringement ("Internet piracy"), by providing more effective remedies against online infringers, counterfeiters and facilitators of such infringement, particularly those who operate extra-territorially, through the use of non-U.S.-based websites;[1]

SPECIFICALLY, the Section supports, in principle, that Congress, in the enactment of any new enforcement mechanisms or remedies to address extra-territorial Internet piracy, do so in ways that—

(1) appropriately balance the interests of, and the respective burdens that would be placed upon, IP rights-holders, Internet businesses, and Internet users;

(2) avoid unduly impeding freedom of speech and expression, retarding the future growth of the Internet, or stifling legitimate innovations in the structure or functionality of the Internet;

(3) establish any new remedies only after taking full account of the impact on the structure or functionality of the Internet and the potential for harm thereto;

(4) absent clear justification, neither expand nor contract existing third party copyright liability, or exceptions and limitations on liability under existing trademark and copyright law; and

(5) provide appropriate penalties (including criminal penalties) on such piracy wherever it would constitute a violation of U.S. laws, and, in particular, would give rise to criminal penalties, had the piracy arisen from a U.S.-based website.

B. Resolution TF-03

RESOLVED, that the IPL Section supports full compliance by the United States with existing treaty obligations, particularly those governing the international treatment of intellectual property rights;

FURTHER RESOLVED, that the IPL Section urges the enactment of legal mechanisms or remedies to address extra-territorial piracy and counterfeiting that target such online infringement and counterfeiting, but only in so far as those mechanisms or remedies are fully compliant with existing treaty obligations.

NOW THEREFORE, the IPL Section urges the enactment of such new enforcement mechanisms and remedies against online copyright and trademark infringers and counterfeiters as well as the facilitators of such activities whose websites operate outside the U.S., but only in so far as such enforcement mechanisms and remedies are fully consistent with existing treaty obligations.

C. Resolution TF-04

Intentionally left blank.

III. DISCUSSION: Defining the Problem of Online Piracy and Counterfeiting

The growth of the Internet and recent technological developments have, in combination with strong intellectual property laws, contributed to the spread of knowledge and information, as well as opportunities for the development of international commerce and communication on a scale previously unimaginable. These technological and legal developments have helped to create a knowledge-based level playing field among countries and territories that otherwise exhibit great differences in economy, culture, and rule of law. Yet the overwhelming benefit of this new frontier, with worldwide freedom to create and disseminate new ideas, new copyrighted works and new trademarks to identify goods and services and the ability to collaborate instantaneously across borders in the spread of information and the transport of goods, has come with some significant strain to copyright and trademark laws, especially in the area of the enforcement of rights. The purpose of this White Paper is to provide information on specific on-line piracy and counterfeiting problems—in particular, enforcement deficiencies not currently available to U.S. rightsholders or enforcement officials, to address Predatory Foreign Websites ("PFWs") that engage in "extra-territorial" piracy and counterfeiting (*i.e.*, occurring outside of the U.S.), and to recommend possible solutions to address these problems in ways that balance the benefits and burdens of strong and effective enforcement with open access and due process concerns of Internet businesses and users.[2]

As the Supreme Court has noted, "copyright supplies the economic incentive to create and disseminate ideas,"[3] and "[a] well-functioning international copyright system would likely encourage the dissemination of existing and future works."[4] Trademark rights, on the other hand, serve two purposes, first, "by preventing others from copying a source-identifying mark, [they] reduce the customer's costs of shopping and making purchasing decisions," and second, "the law helps assure a producer that it (and not an imitating competitor) will reap the financial, reputation-related rewards associated with a desirable product."[5] In other words, trademarks protect consumers from being misled while protecting the goodwill of the entity that owns the mark. Unlike copyrights, which deal with the marketplace of expressive ideas, trademarks deal with the marketplace of goods and services.

Copyright and trademark laws are "territorial," so protection (if any), as well as ownership, rights, exceptions, and remedies, pertaining to the use of any particular protected work or mark is determined by national laws in the territory where the work or mark is being used or exploited. Thus, the terms "international copyright law" and "international trademark law" are misnomers. International copyright and trademark laws and enforcement refer to the inter-connected national copyright and trademark laws, interlaced (and informed) by international treaties and other agreements and obligations. Any "harmonization" of national laws and international norms, including enforcement, are dependent on bilateral, regional and/or other multi-lateral instruments or agreements. The seminal agreements[6] set the basic terms (the "norms") that member countries must provide by way of protection, rights, exceptions, and remedies, for rightsholders and users of works in each member country. However, the specific rights, exceptions, and tools for enforcement of these rights and exceptions, are

found in national laws, such as the U.S. copyright law (title 17) and U.S. trademark law (title 15) and in state laws, as well as in criminal, administrative, and customs codes.

In addition to all of the positive developments, the growth of the Internet has resulted in a dramatic rise in on-line piracy (copyright) and counterfeiting (trademark), especially by large-scale commercial enterprises (including by organized criminal syndicates) engaged in lucrative unauthorized businesses. The services at issue (in this White Paper) are those dedicated to infringing activity. Many of these enterprises are multi-territorial in nature and are "outward" looking, meaning they actively seek users, customers, and revenue from foreign territories.[7] National laws, for example, U.S. copyright law, provide clearly that certain activities of individual users of these unauthorized sites or services are infringing, for example by uploading or downloading unauthorized copyright material, or the unauthorized distribution or dissemination (including public performance), in or from the United States.[8] Other countries similarly make unauthorized uploading and downloading a violation of an exclusive right under their national laws—including by reproduction, distribution, communications to the public, making available, and/or public performance. National laws, such as U.S. copyright, trademark, criminal and other enforcement tools can adequately address the problems of piracy and counterfeiting in the U.S., whether by end-users or by third party liable parties (under existing vicarious, contributory and inducement theories). Additionally, "safe harbors" —— such as limitations on monetary damages, notice and takedown, and other incentives for cooperation (whether by law or private agreement) between online intermediaries and copyright and mark owners —— have proven beneficial to dampen illegal activity and encourage legal activities and services.

Enforcement for activities occurring in the U.S. or abroad is most effective when undertaken against the owners or operators of large-scale commercial enterprises running servers or services, meaning against the enterprises-themselves, not the thousands (or millions) of end-users. For activities occurring abroad, this requires extra-territorial enforcement. Alternatively, for services or enterprises that are not substantially dedicated to infringing activity, but in which some infringing activity is revealed, more cooperative activities, including notice and take-down, appropriate third party liability laws in combination with other remedial steps against end-users, are effective.

A few clarifications are in order. First, it is important to note that nothing in this White Paper suggests any change in U.S. law to existing direct infringement or third party liability law. Also, the purpose of this White Paper is not to suggest additional ways to identify and/or punish or criminalize individual behavior on the Internet, nor to expand or contract existing third party copyright liability or existing exceptions and limitations on trademark liability. Rather, this White Paper is meant to focus on and offer suggested solutions and remedies that would be effective against extra-territorial infringement and counterfeiting. Such solutions or remedies would only address the activities of users in the United States, not those activities in the "host" country, which can only be addressed by national laws. Enforcement of infringing or counterfeiting activity that originates abroad is very difficult and costly to pursue, and even more so for individual creators and mark owners as well as small business owners of copyrights and trademarks.

Additionally, because of the size and scope of extra-territorial infringement and counterfeiting, and the resulting damage caused to rightsholders, existing civil remedies are ineffective, and therefore, law enforcement officials need effective, efficient, and fair, criminal enforcement tools. Law enforcement officials in many countries have difficulty keeping pace with or staying ahead of online trademark counterfeiting and copyright piracy because traditional methods of enforcement are proving ineffective. Not surprisingly, the Internet's worst offenders have creatively adjusted their activities to stay ahead of the law, modifying their business models to avoid liability and, increasingly, locating their operations selectively to avoid jurisdiction.

The most direct approach to effective enforcement of copyright and trademarks, both of which are territorial rights, is for nations to address their own localized large-scale infringement through national criminal laws and enforcement actions. United States lawmakers and enforcement officials have endeavored to do so locally (and to allocate government resources to such enforcement), and abroad via bilateral and multilateral negotiations and discussions with dozens of countries. For more than a decade, legal reform, U.S. court decisions, and enforcement authorities have acted successfully against some of the major U.S. sources of pirated content online using civil, criminal and other remedies.[9] However, large-scale piracy operations accessible within the United States to end-users in (and targeted in) the United States now largely operate internationally. For several years now, the U.S. Immigration and Customs Enforcement ("ICE") agency has aggressively targeted and seized both domestic and foreign owned websites selling counterfeit goods and distributing copyrighted content. ICE's enforcement efforts, however, are limited to those web addresses for which U.S. based registries act as the official registry operator (*i.e.*, a ".com," ".net," ".org," etc.). While the indictment last year against the operators of MegaUpload has set an example that large-scale infringing criminal activities will be policed globally, such international enforcement efforts can only be coordinated in like-minded jurisdictions intolerant to these types of intellectual property crimes. Authorities in the MegaUpload case, coordinating from nine different countries, were able to arrest five of the site's operators in New Zealand and shut down servers in the United States, the Netherlands, and Canada—seizing a total of about $50 million in assets. At the time of this writing, a criminal case was proceeding under New Zealand (and U.S.) law. However, illegal activities that operate from other jurisdictions too rife with corruption, lacking the legal or enforcement infrastructure, or simply lacking the political will to protect legitimate content online, remain out of reach for U.S. law enforcement.[10] It is this type of activity, and the solutions proposed to address these types of problems, that are the focus of this White Paper.

If the Internet creates a level technological playing field and universal access for all of its users, it operates in a governmental playing field that is far from equal across territories. Where criminal enterprises (engaged in large-scale piracy and counterfeiting operations) have found refuge in safe haven countries, they have set up operations that violate U.S. law (and other national laws and international norms), but nevertheless reach the desktops of American (and other foreign) consumers. Some of the worst actors in the Internet infringement arena today operate profitable commercial websites from jurisdictions where enforcement is unattainable and inflict damaging losses on U.S. brands and markets for copyrighted content and brands. The Russia-based social media site vKontakte, recently ranked among the four most visited sites in Russia and among the top 40 most visited websites in the world, offers legitimate services while permitting users to provide access to large quantities of infringing materials (an entire "service" of illegal music, films and television programs—none of which is licensed). Because authorities in Russia have failed to force the illegal activity via vKontakte to stop, the site operates freely, and is accessible in English from the United States. The Pirate Bay, a Sweden-based BitTorrent indexing site that permits massive amounts of unauthorized access to infringing copyrighted material, has escaped closure despite the fact that its operators have been criminally convicted in Sweden. As reported by Alexa.com and highlighted in the U.S. Trade Representative's ("USTR") 2011 Special 301 Out-of-Cycle Review of Notorious Markets, The Pirate Bay recently ranked among the top 100 websites in both global and U.S. traffic. Meanwhile, smaller-scale websites can offer newly released content within the most profitable window of time for rightsholders to recoup their investments, leaving less of a mark individually but collectively causing significant damage. The USTR lists the China-based linking sites Sogou MP3 and Gougou, which direct users to "deep linked" content located on third-party hosting sites that appear and disappear in time frames short enough to cause damage while escaping enforcement measures which naturally take longer.

There are also many similar examples of trademark infringement. For example, there are fewer than 300 government authorized online pharmacies in Canada, but more than 11,000 fake "Canadian" pharmacies operating online from overseas jurisdictions, some of which are based in Russia or India and distribute counterfeit pharmaceuticals produced in China.[11] The World Health Organization (WHO) reports that over 50% of pharmaceuticals sold from sites that conceal their physical address are counterfeit.[12]

The fact that some of the Internet's worst offenders continue to reach U.S. consumers highlights the need for adequate tools (with extra-territorial jurisdiction) to allow U.S. authorities to enforce the laws that govern and protect U.S. authors, creators, producers, and businesses of copyrighted works and trademarked goods, at the same time allowing these same copyright and trademark laws to also protect legitimate users and consumers. Certainly, the basic principles that have permitted the Internet to thrive must be guarded: open commerce, innovation, free expression, privacy, due process, and transparency are all crucial elements to the continued progress of on-line commerce and communications, as well as fair and defensible copyright laws and enforcement mechanisms. At the same time, enforcement capabilities must allow for speedy, agile, and effective measures against sites that prey on the works and marks of U.S. rightsholders from abroad.

The types of activities to be captured by such jurisdiction are varied in size, scope, and nature. While it is tempting to characterize these bad actors by a certain threshold scale of activity or damage caused, some of the smallest-scale of the blatantly infringing web operations, when considered collectively, can do as much damage or more than that inflicted by single bad actors such as VKontakte or The Pirate Bay. The difficult task of this White Paper is to properly define the "bad actors" and to recommend solutions directed at them that are appropriate, effective, and flexible, but that do not over-enforce against legitimate users. In the example of deep linking site activities, authorities might need the flexibility to address either the centralized linking site or, should that site be transient, a long list of small third-party hosted sites that cause collective damage.

The nature of the sites to be covered by such jurisdiction is similarly difficult to pin down, as new forms of online piracy and counterfeiting can form in a matter of days and are sure to continue to proliferate in the future. Just days after the MegaUpload indictment, for example, The Pirate Bay replaced its .torrent files with "magnets"—a previously relatively unknown technology that makes illegal files more difficult to be traced.[13]

The term "rogue website" has gained popularity to describe the illegal servers, services and/or activities meant to be captured by extra-territorial jurisdiction over infringing activity. To borrow a term from another area of enforcement that has faced territoriality concerns, "offshore betting" has earned the connotation of activity that is illegal in the United States but nevertheless can be reached by U.S. residents. The present problem, then, might best be termed "offshore rogue actors," meaning activities or services (not always necessarily traditional websites) that damage U.S. rightsholders and commercial interests but escape U.S. law by taking operations abroad. What they have in common is, strictly speaking, twofold: first, that their activities would be subject to liability under U.S. law and, second, that they are strategically located within territories whose local authorities fail to take action at a level that meets the standards of U.S. enforcement.

The Federal Government has been strategizing ways to fight these forms of on-line piracy and counterfeiting for some time, and House and Senate actions in the past few years bear witness to the complicated nature of the problem and possible solutions, as well as the divisive nature of the debate on any such solutions. Yet, it is estimated, by various government and private sector experts, that intellectual property thefts cost the U.S. economy over $100 billion per year.[14] The goal of this White Paper is to discuss in detail the problem, and proposed solutions with private and/or public

remedies, in ways that adequately, effectively, and efficiently allow for enforcement of copyrights and trademarks, but that do so in a manner that addresses only the "bad" actors and with mechanisms that are fair and respectful of the due process rights of defendants and other innocent Internet businesses and users.

Notes

1. The definition of Predatory Foreign Websites ("**PFWs**") as described on page 8 of this White Paper governs the type of conduct for which the IPL Section seeks redress. The text of this and other resolutions that were drafted before the development of the PFW definition are included here for purposes of historical accuracy.

2. The IPL Section's White Paper focuses on copyright and trademark issues because of the constituent make-up of its membership. There are several other issues to consider, including privacy, network security, and the effective functioning of the Internet, in any legislative formulation, even if they are not specifically addressed at all, or in detail, in this White Paper.

3. Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 558 (1985)

4. Golan v. Holder, 132 S. Ct. 873, 889 (2012).

5. Qualitex Co. v. Jacobson Prods. Co. Inc., 514 U.S. 159, 163-64 (1995).

6. The seminal agreements include the Berne Convention for the Protection of Literary and Artistic Works (Berne), the Paris Convention for the Protection of Industrial Property, the WTO TRIPS Agreement, the WIPO "digital" treaties (the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty), and the Anti-Counterfeiting Trade Agreement (not yet in force). Note, that the White Paper is not addressing nor recommending any solutions that would be inconsistent with U.S. international treaty or agreement obligations. Rather, it is trying to seek solutions for "effective action" against infringement of intellectual property rights, as for example, called for in the WTO TRIPS Agreement ("fair and equitable" and "shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays"). Article 41(1)(2).

7. It should also be noted that many American consumers intentionally seek out these illegal services. The more legal services and better distribution models with broader availability of legitimate content continue to develop and thrive, the more consumers will, hopefully, turn away from illegal services. This White Paper does not address the development of new legal services or business models; rather, it focuses on remedies against the services or sites doing significant economic harm to rightsholders, in the hope that stopping these "bad actors", or PFWs, can create a business environment for more and better legitimate services to flourish.

8. A&M v. Napster, 239 F.3d 1004, 1014 (9th Cir. 2001) ("Napster"): "Napster users infringe at least two of the copyright holder's exclusive rights…reproduction…[and] distribution" and noting that Napster "pretty much acknowledged [this]"); *In re* Aimster Copyright Litigation, 334 F.3d 643, 645 (7th Cir. 2003) ("Aimster") ("such swapping [using Aimster/Madster service], which involves making and transmitting a digital copy of the music, infringes copyright"); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1034-35 (C.D. Ca. 2003), *aff'd by* 545 U.S. 913 (2005) ("Grokster") ("it is undisputed that…" reproduction and distribution rights are infringed by some end-users).

9. *See e.g.,* Napster, Aimster, Grokster, Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481 (S.D.N.Y. 2010) ("LimeWire"). See also Disney Enterprises, Inc. v. Hotfile Corp., Case No. 11-20427-CIV-WILLIAMS, 2013 WL 6336286 (S.D.Fla., Sep. 20, 2013) (available at http://ia600408.us.archive.org/18/items/gov.uscourts.flsd.373206/gov.uscourts.flsd.373206.534.0.pdf) ("*Hotfile*") (granting summary judgment for plaintiff movie studios against a defendant "storage locker" service on the grounds that defendant was vicariously liable for the infringements of its users and that defendant was not entitled to the DMCA's "safe harbor").

10. There have been a few notable exceptions: in October 2013 the illegal website isoHunt.com ceased operations and agreed to a settlement of $110 million with rightsholders. This resolution came after seven years of litigation and the issuance of a permanent injunction by the district court and the Ninth Circuit. The illegal BitTorrent website had continued its operations even after the district court's injunction in 2009 because of the territorial limits of enforcement—the website was operated from private servers in Canada. *See* MPAA Press Release (Oct. 17, 2013) (available at http://www.mpaa.org/resources/52c16680-37ab-4f0a-9756-b850fe37ca1c.pdf); *see also* Columbia Pictures Indus. et.al. v. Fung, No. 10-55946, 2013 U.S. App. LEXIS 5597 (9th Cir. Mar. 21, 2013) (upholding, but modifying, a permanent injunction against the Canadian website).

11. *See, e.g.,* Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad, National Intellectual Property Rights Coordination Center (Nov. 2011) http://www.iprcenter.gov/reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf.

12. "Medicines: spurious/falsely-labeled/ falsified/counterfeit (SFFC) medicines," World Health Organization Fact Sheet 275 (Jan. 2010) (http://www.who.int/mediacentre/factsheets/fs275/en/index.html).

13. Duncan Green, *Pirate Bay to abandon .torrent files for magnet links*, ArsTechnica, Jan. 2012, http://arstechnica.com/tech-policy/news/2012/01/pirate-bay-to-abandon-torrent-files-for-magnet-links.ars. The site also changed its TLD (top level domain name) from .org to .se, likely to evade jurisdiction and enforcement.

14. For instance, Chairman Lamar Smith explained that "[t]he theft of America's intellectual property costs the U.S. economy more than $100 billion annually and results in the loss of thousands of American jobs." (available at http://lamarsmith.house.gov/media-center/press-releases/statement-from-chairman-smith-on-sopa); *see also* GAO Report on Intellectual Property, "Federal Enforcement Has Generally Increased, but Assessing Performance Could Strengthen Law Enforcement Efforts" (Mar. 2008) (available at http://www.gao.gov/new.items/d08157.pdf) (citing 2007 Org. for Econ. Coop. & Devel., study called "The Economic Impact of Counterfeiting and Piracy" which estimated the value of international theft of IP at $200 billion).

Chapter 1

FORUM SELECTION

I. SECTION POSITION

The IPL Section favors jurisdiction in the U.S. district courts for any new enforcement mechanisms that address online extra-territorial piracy and counterfeiting of U.S. intellectual property rights undertaken by PFWs.

II. SECTION RESOLUTION: TF-05

RESOLVED, that the IPL Section urges Congress, in the enactment of any proposed new enforcement mechanisms that address online extra-territorial piracy and counterfeiting of U.S. intellectual property rights, to vest jurisdiction of actions seeking civil or criminal remedies in the U.S. district courts.

III. DISCUSSION: Online Piracy & Counterfeiting: Forum Selection

A. Jurisdictional Issues

One of the goals of extra-territorial online piracy legislation is to enable intellectual property owners to obtain speedy, efficient, and full relief against violators of their intellectual property. The IPL Section thus considered which forum for resolution of online piracy and counterfeiting actions would best achieve this goal: Article I executive branch agencies (such as the International Trade Commission)[1] or Article III U.S. district courts. The IPL Section did not focus on the jurisdictional limits of any particular available forum, because that could be amended through legislation.[2]

1. Article I—Executive Branch Agencies

Certain executive branch agencies have the advantage of possessing enforcement capabilities (*e.g.*, the Department of Justice) or having relationships with other executive branch agencies that possess enforcement capabilities (*e.g.*, the International Trade Commission and its relationship with Customs and Border Protection). Executive branch agencies also have the advantage of possessing nationwide jurisdiction, unconstrained by geographical limitations within the United States.[3]

On the other hand, most executive branch agencies are limited in the scope of their enforcement authority.[4] They can only perform the functions expressly authorized by their enabling statutes.[5] They may levy fines or sanctions payable to the U.S. government,[6] but that does not remedy the losses that the intellectual property owner may have incurred as a result of the infringement, as they do not have the power to award damages to the intellectual property owner.[7] In addition, any amounts collected are not likely to be high enough to attract the attention of the Attorney General or the U.S. Attorneys' Office, such that enforcement by a prosecutor would be an option.[8] This suggests that executive branch agencies may not be adequate fora to adjudicate online extra-territorial piracy actions.

Congress or the executive branch could, however, augment or amend the jurisdiction and mission of these agencies. As a result, the current limitations on the jurisdiction and scope of current executive branch agencies do not necessarily mean that they are inherently inappropriate fora for

adjudication of extra-territorial piracy actions. For instance, the International Trade Commission now has a record number of pending investigations occupying its time and attention. In Fiscal Year 2011, the ITC instituted 70 Section 337 investigations, the most it has ever instituted;[9] and in FY 2012, the ITC has already instituted 31 investigations.[10] Thus, as things now stand, proceeding before the ITC is not an efficient option for expedited extra-territorial piracy actions. But if Congress were to designate the ITC as the appropriate forum, it could allocate additional funds, staff and/or other resources to support the expected increased volume of cases.

2. Article III—U.S. District Courts

Unlike executive agencies, Article III courts do not have their own enforcement arms,[11] and they have to rely on private parties or governmental entities to initiate civil or criminal proceedings before them. However, once such proceedings are instituted, Article III district courts can enjoin certain conduct and/or award monetary damages to intellectual property owners.[12] They can also adjudicate criminal charges that the U.S. Attorney brings against alleged violators of intellectual property rights.[13]

B. Convenience and Accessibility

1. Article I—Executive Branch Agencies

The responsibility for intellectual property rights enforcement is currently divided among certain executive branch agencies, such as the ITC, the Court of International Trade ("CIT"), the Department of Justice ("DOJ") and Customs and Border Protection ("CBP").[14] Entrusting the responsibility for adjudicating extra-territorial online piracy actions with a single centralized agency, however, would yield several benefits. One benefit is that the hearing officers (likely administrative law judges appointed under the Administrative Procedure Act, 5 U.S.C. §§501 et seq.) would obtain a great deal of experience in these actions. Moreover, a single agency could provide streamlined and expedited proceedings, unlike district courts, which must first attend to their criminal dockets with speedy trial requirements.[15]

There are, however, several drawbacks to centralizing the adjudication of these actions in one agency. Many executive branch agencies are physically located in Washington, D.C., or have only a few locations in the United States. This would increase the burden on intellectual property owners and alleged violators, who would be forced to travel to a centralized location for adjudication of the dispute.[16] This could have a particularly adverse effect on smaller entities and impecunious individuals.[17]

2. Article III—U.S. District Courts

Unlike some executive agencies, Article III district courts are located throughout the United States, allowing relatively convenient access to *fora* for adjudication of extra-territorial online piracy actions.[18] An intellectual property owner could proceed in any convenient U.S. district court that satisfies personal jurisdiction and venue requirements.

District courts also have a common set of procedural and evidentiary rules, regardless of the geographic location of the district court.[19] District courts already handle copyright infringement cases under 17 U.S.C. §501 and counterfeiting actions under 15 U.S.C. §1116. Also, they have handled *in rem* actions against foreign domain names for over a decade under the existing legislation. 15 U.S.C.§1125(d). As a result, there are already decades of preexisting case law that demonstrate how district courts handle piracy and counterfeiting issues[20] which would also allow for the same basic relief to be available in any of the district courts. [21] Consistency in rulings

among the courts would be promoted by developing a body of precedents at the district and circuit court level.

Despite these benefits, there are some drawbacks to using district courts. For instance, district courts could be cost-prohibitive for smaller intellectual property rights owners and may be intimidating for intellectual property rights owners without counsel; especially if the costs of proceeding in these cases mirrored the costs of filing other intellectual property cases.[22]

C. Parallel Proceedings

The IPL Section has also considered the possibility of parallel actions regarding extra-territorial online piracy actions. By way of example, the OPEN Act bill would place jurisdiction for extra-territorial online piracy actions solely in the ITC.[23] However, as explained earlier, the ITC does not have criminal jurisdiction or the ability to award damages.[24] Therefore, in order to obtain comprehensive relief for intellectual property owners, those owners would be forced to approach the U.S. Attorney's Office regarding possible criminal prosecution while also pursuing parallel civil litigation against the alleged infringers.

The concept of parallel litigation is currently available in patent infringement proceedings. Specifically, in the context of Section 337 investigations at the International Trade Commission, complainants often file parallel actions in the U.S. district court so that they can obtain not only the injunction relief available through the ITC, but also any monetary relief available through the U.S. district courts. In other words, a plaintiff in this situation would file two lawsuits (one in the ITC and the other in district court) in order to obtain both injunctive and monetary relief in a case that presumably justifies both types of relief.[25] A district court must stay the case before it, pending a parallel proceeding in the ITC. 28 USC §1659(a).[26] If an intellectual property owner is forced to pursue such parallel actions in order to combat extra-territorial online piracy actions, then those costs may be prohibitive for small or solo intellectual property owners.[27]

D. Expedited Proceedings

In order to help alleviate intellectual property owners' concerns about the cost of pursuing district court actions against extra-territorial online piracy, the IPL Section recommends using expedited proceedings, such as preliminary injunction proceedings. Such proceedings already exist in the Federal Rules and are regularly used in trademark infringement cases.[28] Expedited proceedings would reduce the costs of enforcement and also reduce concerns that normal procedural rules might be too slow to contend with foreign infringers who change domain names and websites nearly instantaneously.

E. Protections against Misuse

The IPL Section recommends vesting the U.S. district courts with jurisdiction over extra-territorial online piracy and counterfeiting actions because the Federal Rules of Civil Procedure (FRCP) provide protection against abusive litigation. Under FRCP 65(c), an intellectual property owner bringing such an action could be required to post a security bond. Under FRCP 11, an intellectual property owner who brings frivolous actions could be subject to sanctions.[29] Vesting jurisdiction in the district courts would place the litigants under these and other existing rules that limit the risk of false or intentionally misleading claims being presented.

IV. CONCLUSIONS

The IPL Section recommends that extra-territorial online piracy actions be brought in Article III U.S. district courts. District courts bring the broadest scope of experience in intellectual property

law and the broadest potential set of remedies available. Appropriate remedies could include injunctive relief, damages and/or criminal sanctions, all of which are within a district court's ability to adjudicate and award.[30] District courts can also adjudicate criminal enforcement actions, which Article I executive branch agencies are prohibited (on Constitutional due process grounds) from adjudicating. District courts have had decades of experience in copyright piracy and trademark counterfeiting cases. While these are new permutations to an existing problem, the underlying dilemma is the same. Jurisdiction over online intellectual property infringement matters should be vested in the district courts, which have the experience in dealing with similar matters. Similarly, the Department of Justice and the U.S. Attorney's offices throughout the United States have extensive experience prosecuting criminal actions against foreign websites. This experience should be used in prosecuting foreign online counterfeiters and cyber pirates. Finally, the IPL Section recognizes that expedited proceedings are necessary to give intellectual property owners an appropriate and speedy mechanism to address extra-territorial online piracy and counterfeiting (while ensuring the due process rights of the web sites being targeted).

Notes

1. This option was suggested in the OPEN Act, introduced separately during the 112th Congress by Sen. Wyden and Rep. Issa, as S. 2029 and H.R. 3782, respectively.

2. Parties would appeal decisions of the U.S. district courts or the International Trade Commission to the U.S. Court of Appeals for the Federal Circuit. Therefore, the IPL Section considered this factor to be neutral.

3. *See, e.g.*, 19 U.S.C. §1333(b) (1990) (authorizing nationwide service of process for witnesses and evidence in ITC investigations); 28 U.S.C. §533 (2002) (authorizing the Department of Justice to investigate acts against the United States).

4. *See* About the ITC, http://www.usitc.gov/press_room/about_usitc.htm (last visited Sept. 23, 2013); *The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, SEC.GOV, http://www.sec.gov/about/whatwedo.shtml (last visited Sept. 23, 2013).

5. *See* 2 Am. Jur. 2d Administrative Law §54.

6. *See, e.g.*, 47 U.S.C. §503(b) (2010) (authorizing FCC to impose "monetary forfeitures" (fines) on licensees for violations of the Act); *see also* 15 U.S.C. §78f (2010) (authorizing SEC to impose sanctions upon a finding of violation).

7. *See, e.g.,* http://www.copyright.gov/docs/regstat032906.html (last visited Sept. 23, 2013) (Statement of the U.S. Copyright Office before the Subcommittee on Courts, the Internet, and Intellectual Property, Committee on the Judiciary regarding the high cost of litigation for small or solo copyright holders).

8. Statement of John Morton, Director of U.S. Immigration and Customs Enforcement, Before the U.S. House of Representatives, Committee on the Judiciary, at 15 (Apr. 6, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Morton04062011.pdf).

9. *See FY 2011 Highlights: USITC Sees Record Number of Intellectual Property Infringement Cases Filed*, USITC.GOV (available at http://www.usitc.gov/press_room/documents/featured_news/337_timeframes_article.htm).

10. *Section 337 Statistical Information*, USITC.GOV (available at http://www.usitc.gov/press_room/337_stats.htm).

11. *Federal Courts in American Government* (available at http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/FederalCourtsInAmericanGovernment.aspx).

12. *See* http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/DistrictCourts.aspx.

13. *Id.*

14. *See* About the ITC (available at http://www.usitc.gov/press_room/about_usitc.htm); *About the Court*, CIT.USCOURTS.GOV (available at http://www.cit.uscourts.gov/AboutTheCourt.html); *Department of Justice Agencies*, JUSTICE.GOV (available at http://www.justice.gov/agencies/index-list.html); *We are CBP!*, CBP.GOV (available at http://www.cbp.gov/xp/cgov/careers/customs_careers/we_are_cbp.xml).

15. *See* 18 U.S.C. §3161; 3B FED. PRAC. & PROC. CRIM. §833 (3d ed. 2012) (The Speedy Trial Act).

16. *See, e.g.,* Report to Congress; Trademark Litigation Tactics and Federal Government Services to Protect Trademarks and Prevent Counterfeiting, at 24-25 (April 2011) (available at http://www.uspto.gov/trademarks/

notices/TrademarkLitigationStudy.pdf); *see also* Small Business Regulatory Enforcement Fairness Act of 1996, Sec. 202 ("small business bear a disproportionate share of regulatory costs and burdens"); *see also* Statement of the U.S. Copyright Office before the Subcommittee on Courts, the Internet, and Intellectual Property, Committee on the Judiciary regarding the high cost of litigation for small or solo copyright holders (available at http://www.copyright.gov/docs/regstat032906.html).

17. Report to Congress; Trademark Litigation Tactics and Federal Government Services to Protect Trademarks and Prevent Counterfeiting, at 24-25 (April 2011) (available at http://www.uspto.gov/trademarks/notices/TrademarkLitigationStudy.pdf); *see also* Small Business Regulatory Enforcement Fairness Act of 1996, Sec. 202 ("small business bear a disproportionate share of regulatory costs and burdens").

18. *See* http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/DistrictCourts.aspx.

19. *See* Fed. R. Civ. P. 1; Fed. R. Evid. 101, 1001.

20. *See* Lorillard Tobacco Co. v. Bisan Food Corp., 377 F.3d 313 (3d Cir. 2004) (ruling upon district court's findings under Trademark Counterfeiting Act of 1984, 15 U.S.C. §1116(d)) (1984)); Levi Strauss & Co. v. Shilon, 121 F.3d 1309, 1312 (9th Cir. 1997) (ruling upon district court's findings under §32 of the Lanham Act, 15 U.S.C. §1114).

21. *See* Fed. R. Civ. P. 1; *see, e.g.*, 28 U.S.C. §1400(b) (1999).

22. *See, e.g.,* Report to Congress; Trademark Litigation Tactics and Federal Government Services to Protect Trademarks and Prevent Counterfeiting, at 24-25 (April 2011) (available at http://www.uspto.gov/trademarks/notices/TrademarkLitigationStudy.pdf); *see also* Small Business Regulatory Enforcement Fairness Act of 1996, Sec. 202 ("small business bear a disproportionate share of regulatory costs and burdens"); Statement of the U.S. Copyright Office before the Subcommittee on Courts, the Internet, and Intellectual Property, Committee on the Judiciary regarding the high cost of litigation for small or solo copyright holders (available at http://www.copyright.gov/docs/regstat032906.html).

23. *See* S. 2029, 112th Cong. (2011); H.R. 3782, 112th Cong. (2011).

24. *See* The U.S. International Trade Commission, Section *337 Investigations: Answers to Frequently Asked Questions*, Pub. No. 4105 (Mar. 2009) (available at http://www.usitc.gov/intellectual_property/documents/337_faqs.pdf).

25. Schaumberg, A Lawyer's Guide to Section 337 Investigations before the International Trade Commission, at 201.

26. 28 U.S.C. §1659 (2007).

27. *See, e.g.,* W. Mark Crain, *The Impact of Regulatory Costs on Small Firms*, U.S. Small Business Administration, Office of Advocacy (Sept. 2005) (available at http://archive.sba.gov/advo/research/rs264tot.pdf); Report to Congress; Trademark Litigation Tactics and Federal Government Services to Protect Trademarks and Prevent Counterfeiting, at 24-25 (April 2011) (available at http://www.uspto.gov/trademarks/notices/TrademarkLitigationStudy.pdf); *see also* Small Business Regulatory Enforcement Fairness Act of 1996, Sec. 202 ("small business bear a disproportionate share of regulatory costs and burdens"); *see also* Statement of the U.S. Copyright Office before the Subcommittee on Courts, the Internet, and Intellectual Property, Committee on the Judiciary regarding the high cost of litigation for small or solo copyright holders (available at http://www.copyright.gov/docs/regstat032906.html) .

28. 15 U.S.C. §1116 (providing for injunctive relief against trademark infringement); *see, e.g.,* Suzuki Motor Corp. v. Jiujiang Hison Motor Boat Mfg. Co., Ltd., No.: 1:12-cv-20636.2012 WL 640700 (S.D. Fla. Feb. 27, 2012) (granting motion for preliminary injunction in trademark infringement suit).

29. *See* Phonometrics, Inc. v. Economy Inns of America, 349 F.3d 1356, 1365 (Fed. Cir. 2003) (affirming district court's grant of sanctions under Rule 11 based on filing of frivolous patent-infringement claim); Colida v. Nokia Inc., No. 07 Civ. 805, 2008 WL 4449419, at *2 (S.D.N.Y. Sept. 29, 2008) (granting Rule 11 sanction based on filing frivolous patent-infringement claim).

30. The Civil Remedies section of this White Paper addresses the benefits and limitations of remedies that can be awarded in these cases, and recommends can be made about the type of relief that would be appropriate for these types of matters.

Chapter 2

CIVIL REMEDIES

I. SECTION POSITION

The IPL Section favors the imposition of civil remedies against websites that are judicially determined to be Predatory Foreign Websites ("PFWs"). The Section also favors injunctive relief and monetary damages against U.S.-based intermediaries that support the operation of PFWs and do not voluntarily take action to redress online piracy and counterfeiting by PFWs.

II. SECTION RESOLUTION: TF-06

RESOLVED, the IPL Section supports the imposition of certain civil remedies following a judicial determination that online piracy and/or counterfeiting has been undertaken by specifically-named online copyright pirates and/or trademark counterfeiters who operate through websites whose non-U.S. locational elements (as to, *e.g.*, operators, hosts and/or domain names) make it difficult to enforce U.S. law against but that are accessible in the U.S. and that are targeted at U.S. consumers ("Predatory Foreign Websites"), as well as the facilitators of such activities; and

FURTHER RESOLVED, the IPL Section supports the supplementation of the following civil remedies (which are already available under U.S. law to redress piracy and/or counterfeiting that occurs within U.S. borders) to redress online piracy and counterfeiting undertaken by Predatory Foreign Websites, in cases where the intermediary(ies) in question does not take action voluntarily:

1) injunctions directing financial payment processors to freeze the assets of Predatory Foreign Websites and to cease doing business with such websites;
2) injunctions preventing online advertisers from paying Predatory Foreign Websites or from displaying further ads on those websites;
3) injunctions requiring search engines to remove Predatory Foreign Websites from paid, sponsored links;
4) injunctions requiring website hosts to cease hosting Predatory Foreign Websites;
5) injunctions permitting the seizure and destruction of counterfeit or pirated goods, or their delivery to rightsholders who are willing to bear the shipping and handling costs;
6) injunctions requiring the immediate removal of pirated works and/or content, counterfeit marks, logos, insignia, or trade dress that have been made available, displayed, or otherwise promoted by such online pirates and/or counterfeiters on Predatory Foreign Websites; and
7) monetary damages in the form of disgorgement of profits of the Predatory Foreign Websites achieved as a result of the illegal activity, which shall be paid to the rightsholder from the assets frozen or advertising/sponsored links revenue that had been withheld by the intermediaries, as described in 1)—3) above.

FURTHER RESOLVED, the IPL Section supports the development of a comprehensive public outreach program intended to educate the public about recognizing and avoiding pirated works and/or content or counterfeit goods, and about the negative impacts that online piracy and counter-

feiting have on the U.S. economy, in an effort to decrease public traffic to Predatory Foreign Websites.

NOW THEREFORE the IPL Section supports the supplementation of existing injunctive relief and monetary damages to redress online piracy and counterfeiting undertaken by Predatory Foreign Websites and to return the pirated works and/or content or the counterfeit goods (or require their destruction), at the discretion of the owner of the intellectual property rights that were harmed by the illegal activity.

III. DISCUSSION

A. Background

This White Paper seeks to provide guidance to Congress in establishing remedies for civil litigants seeking redress against foreign-based websites engaged in online piracy and counterfeiting that is currently beyond the reach of the Copyright Act or the Lanham Act.

The primary obstacle to redressing online piracy and counterfeiting of this type is that it originates in foreign nations beyond the sovereign jurisdiction of the United States. Popular destinations for pirated content are registered, hosted, and operated outside the reach of United States law.[1] Likewise, counterfeiters operate websites that reach U.S. consumers, but, by being registered, hosted, and operated abroad, attempt to avoid U.S. jurisdiction.

Such websites do not operate in a vacuum. To reach their customers and (in the case of revenue-generating websites) to make money from them, foreign websites rely upon a host of intermediaries, many of them within the boundaries of U.S. jurisdiction, who provide a variety of vital services: financial, advertising, logistical, and otherwise. If U.S. legislation enabled litigants to identify and cut off such websites' access to the services of these intermediaries, U.S. courts could help curtail foreign online counterfeiting and piracy via an indirect route. But to avoid overbreadth and unintended spillover effects, any such legislation much carefully define the types of foreign websites that would be subject to such court actions, and the types of intermediaries who would be asked to cut off services to such sites.

1. Definition of Predatory Foreign Websites (PFWs)

This White Paper uses the phrase "Predatory Foreign Websites" or "PFWs" to refer to websites engaged in the type of conduct sought to be remedied, but recognizes that sponsors of prior versions of legislation introduced in Congress have used different phrases to describe this conduct, without establishing a universal definition.[2]

This White Paper makes no attempt to choose any particular definition of this phrase, but instead seeks only to address the limited category of foreign-originated websites engaged in large-scale piracy of U.S. copyrighted content (in this case, any work created in the U.S., covered by the Copyright Act, capable of dissemination through electronic means) or counterfeiting of U.S. trademarks (in this case, intentional use of a spurious trademark that is identical to or substantially indistinguishable from an authentic trademark, in connection with products that are not from by the trademark owner or its agent). In particular, while the conduct itself may be identical to that prohibited under existing law, these specific actions are not readily subject to adjudication in the U.S. because the website is either beyond the jurisdiction of U.S. enforcement authorities entirely or, even if technically subject to such jurisdiction, is beyond the reach of such authorities to enforce a judgment against them. This limited scope of illegal conduct is the focus of this White Paper.

By way of further clarification, this White Paper does not attempt to pull within the definition of "Predatory Foreign Websites" any sites that are already subject to U.S. jurisdiction under existing U.S. law or other treaty obligations, and specifically excludes those sites from this analysis.

a) Predatory Foreign Websites engaged in Copyright Infringement

Consider a website hosting pirated copyrighted content. It is based abroad, in a locale where the government is not friendly to U.S. intellectual property interests. The website uses a foreign domain. What remedies are available to stop this pirated copyrighted material? What remedies should be available?

Remedying foreign-based copyright piracy is difficult and there are no easy solutions. A promising approach involves following the money.[3] If the flow of money to these Predatory Foreign Websites dries up, the expectation is that the websites themselves may cease operations.

Predatory Foreign Websites generate revenue primarily in two ways: selling advertising and selling access to pirated content.[4] Both of these revenue streams can be closed by providing a standardized means for rightsholders to seek court orders requiring advertising services and payment providers to stop accepting payments from, or issuing payments to, these sites.

Unfortunately, providing a mechanism for rightsholders to cut off a Predatory Foreign Website's access to revenue does not address the problem of Predatory Foreign Websites that operate entirely for free; for example, a website that distributes pirated content without fee or advertising. Such sites may yet still make a significant impact on the market for legitimately acquired copyrighted works. Because there is no money to follow, a "follow the money" strategy would not address these sites. For Predatory Foreign Websites that do not rely on revenue from U.S. intermediaries,[5] technical solutions, though controversial, are available.

One technical solution would require U.S. ISPs to block their users' access to such sites through techniques such as DNS blocking or IP address blocking.[6] Though such techniques are expressly provided for under U.S. copyright law[7] and are used in a number of jurisdictions outside the U.S.,[8] they have generated significant Internet security[9] and First Amendment concerns.[10]

Another technical solution would require search engines to cease indexing and returning search results from such sites, upon notification by a rights-holder or otherwise. Many of the same First Amendment concerns raised in response to the site-blocking provisions of PIPA/SOPA were also raised with regard to the bills' provisions on search engine de-indexing,[11] although there were some voices who opposed site-blocking but supported de-indexing, at least under some conditions.[12]

To date, the IPL Section has not reached consensus on either of these technical solutions, or any other potential remedy that addresses sites that do not receive revenue from U.S. intermediaries. Consequently, the balance of this White Paper will solely address sites that receive revenue from U.S. intermediaries.

What about websites that might have legitimate content alongside pirated content? Ideally, narrowly targeted remedies would focus on only addressing money made from pirated content, leaving legitimate aspects of a website untouched. However it is impractical, if not impossible, to identify which revenues earned by a site (*e.g.*, advertising or subscription income) are derived from the lawful, as opposed to the unlawful, content available on the site. Moreover, proponents recognized the line-drawing difficulties associated with triggering enforcement mechanisms against sites with substantial quantities of legitimate content. For both reasons, prior legislation introduced to combat Predatory Foreign Websites has focused only on near-total piracy on com-

pletely illegitimate sites, thereby avoiding affecting sites with legitimate purposes even if some of their content was pirated.[13]

At the same time, there is a distinct concern about due process. Obviously, foreign websites that are not breaking applicable law should not be adversely affected by U.S. legislation. Rightsholders should not be granted tools without safeguards to prevent abuse. Care needs to be taken to ensure due process is respected, because a legitimate website taken down by mistake would struggle to recover, if it ever recovered at all.[14]

For the purposes of stopping copyright piracy by Predatory Foreign Websites, this White Paper focuses on:

- foreign-hosted sites with either foreign (*e.g.*, .cn, .ru, .se, etc.) or domestic domains (.com, .org, .biz, etc.);[15]
- with some form of revenue (ad-based or direct-pay); and
- evidence[16] of knowledge by the Predatory Foreign Website of substantial infringing content being present on its site.

b) Predatory Foreign Websites engaged in Trademark Counterfeiting

The rise of Internet shopping means that the old way of counterfeiting—large shipments that could be intercepted and inspected at the border—has made way for a new, direct-to-consumer model that makes it much more difficult to trace and stop the influx of counterfeited goods into the United States. Counterfeiting websites now appeal directly to consumers. Consumers interested in buying counterfeited products can very easily find online stores (either through organic search results or sponsored links, or any other source) willing to sell them.

The sale of counterfeit goods on the Internet is significantly different from online copyright piracy.[17] Goods are real, tangible objects. Counterfeits are physical and consequently cost money to produce and distribute, compared to pirated works, which can be infinitely duplicated and redistributed with little to no cost to the distributor. Unlike copyright piracy, which is sometimes non-commercial, trademark counterfeiting almost necessarily involves a commercial transaction.

As a consequence, "following the money" is almost certainly an effective means of combating websites dedicated to the sale of counterfeit goods. For example, if payment providers and advertising services terminate services to Predatory Foreign Websites involved in the sale of counterfeit goods, those websites would be unable to promote and sell their products online.

For the purposes of stopping trademark counterfeiting, this White Paper focuses on:

- foreign-hosted sites with either foreign (.cn, .ru, .se, etc.) or domestic domains (.com, .org, .biz, etc.);[18]
- with some form of revenue (ad-based or direct-pay); and
- evidence[19] of knowledge by the Predatory Foreign Website of substantial counterfeits being offered on its site.

2. Definition of Intermediaries

For purposes of this White Paper, the term "intermediaries" refers to third parties that are involved in the advertising, distribution, or financial processing aspects of online sales.

a) Financial Providers

Payment services (*e.g.* PayPal), credit card companies (*e.g.* Visa, MasterCard), and banks all serve as intermediaries for websites that earn revenue. Whether the revenue comes from direct sales or from

ad revenue, payment will necessarily pass through a financial provider before arriving in the website owner's accounts. This is true whether a website is connected to a legitimate business or to the distribution of counterfeits or pirated content offered by a Predatory Foreign Website, or anything in between. However, there are many financial providers, and even within a single financial provider's network, there can be thousands of cooperating financial institutions.[20]

b) Advertising Networks

Advertising networks (*e.g.*, Google AdSense) place ads on foreign websites and in turn provide those websites a payout, based on clickthroughs or ad impressions. The Internet Advertising Bureau's semiannual report on Internet advertising revenues (conducted by PriceWaterhouseCoopers) recently reported that "Internet advertising revenues for the first quarter of 2012 set a new record for the reporting period at $8.4 billion," which represents the highest first quarter revenue ever measured and a 15% increase over the Internet advertising revenues reported in the first quarter 2011.[21] The IAB concluded that this dramatic increase in ad revenues was directly related to an increased use of social media and other interactive websites by users around the globe.[22]

Notably, the IAB also reported that over 70% of all Internet advertising revenue was concentrated among the top ten ad selling agencies, while an additional 20% was spread among 40 additional agencies.[23] By far, the largest portion of ad revenues resulted from search-based advertisements, totaling 46.5% of the revenues overall in 2011.[24]

Because of this advertising model, websites can earn revenues even if they do not charge for their content or for access to their sites.[25]

c) Search Engines

Search engines (*e.g.*, Google Search, Microsoft Bing) drive traffic to websites by listing websites in the search results. Some of these are organically generated[26] while some are the result of paid advertisements.

These paid advertisements include keyword-based ads—also called "sponsored links"—which appear alongside or above organic search results (*e.g.*, Google AdWords, Microsoft adCenter).[27] Just like any other purchaser of sponsored links, Predatory Foreign Websites can purchase ads and have them display when consumers search for a particular set of keywords.[28]

Trademark owners concerned about counterfeit websites purchasing sponsored links from Google or other search engines to display when a user searches for their trademarks can submit a web form[29] to request a take down of sponsored links that display misappropriated trademarks.

d) DNS Registrars

Domain name service providers (*e.g.*, NameCheap, GoDaddy, Network Solutions, Domains by Proxy, etc.) serve as registrars for domain names, enabling visitors to use a domain name instead of an IP address to access a website.

e) Internet Service Providers

Internet service providers (*e.g.*, Comcast,[30] Verizon[31]) enable consumers to access the Internet and may provide other services not relevant to this White Paper.

f) Webhosts

Services offered by website hosting companies can vary greatly, but these generally include "provid[ing] space on a server owned or leased for use by clients, as well as providing Internet

connectivity, typically in a data center."[32] Website owners generally pay website hosts for hosting expenses (storage space, bandwidth, CPU time), although there are some hosts that offer basic services for free.[33]

g) Shippers and Carriers

Counterfeiting historically involved bulk shipments of counterfeit goods via container or freight shipping services.[34] The very size of the shipments made it easier for Customs & Border Protection to identify and seize the counterfeit goods. In the wake of increased online shopping activities, consumers frequently order goods directly from online retailers, including Predatory Foreign Websites, and the resulting shipments are more difficult for CBP to identify, as the shipping packages resemble other shipments from legitimate sources and may, in fact, be sent through legitimate multinational carriers (such as Federal Express, UPS or DHL), which handle the delivery to the U.S. consumer.

B. Potential Liability of Predatory Foreign Websites and Intermediaries—Copyright

1. Potential Liability of Predatory Foreign Websites—Copyright

As noted, this White Paper excludes from the definition of "Predatory Foreign Website" all sites that are subject to jurisdiction in the United States under existing U.S. law or other treaty obligations. If a Predatory Foreign Website were subject to enforceable jurisdiction under U.S. law, [35] the copyright owners would have potential claims against such a site for both the site's own direct acts of infringement ("direct liability"), and the site's role in facilitating and supporting direct infringements committed by others, including most notably the site's users ("secondary liability"). This Section addresses copyright owners' potential direct and secondary liability claims against Predatory Foreign Websites. Potential claims that could be made by trademark owners are discussed in Section III below.

Although copyright owners likely would have strong claims against Predatory Foreign Websites, there are practical and legal challenges to asserting such claims in the U.S. In the first place, it is sometimes difficult for rights owners to locate the operators of such sites. And, even where they can be located, such sites likely would raise jurisdictional challenges to a suit based on a violation of U.S. copyright law. Section D discusses some of these issues.

a) Direct Liability of Predatory Foreign Websites—Copyright Law

"To prove a claim of direct copyright infringement, a plaintiff must show that s/he owns the copyright and that the defendant himself violated one or more of the plaintiff's exclusive rights under the Copyright Act."[36] The range of infringing conduct that takes place through Predatory Foreign Websites implicates numerous exclusive rights. An individual site may be responsible for the infringement of more than one exclusive right with respect to the same conduct. We discuss each of these rights in turn.

(1) Right of Reproduction

The owner of copyright under U.S. law has the exclusive right to make copies of his or her work.[37] The activities occurring through many Predatory Foreign Websites involve the direct, unauthorized reproductions of copyright owners' works. Peer-to-peer services, for example, involve the making of a copy on the computer hard drive of the person downloading the file. Sites that stream—or that link to other sites that host—infringing content also will utilize unauthorized copies of copyrighted works that are copied to one or more computer servers.

Civil Remedies

Whether the Predatory Foreign Website will be directly liable for violating the copyright owner's exclusive rights depends upon whether that site is found to be making the unauthorized reproductions. If the site is not doing the copying, but rather is facilitating or encouraging individual users' or other websites' copying, then the basis for the Predatory Foreign Website's liability would be secondary, not direct.

A clear case where a website would be directly liable for unauthorized copying would exist where the site itself placed copies of copyrighted works on its own servers. In that case, the site itself would be liable for the infringement of each work that it copied to its servers.[38]

Predatory Foreign Websites typically do not themselves "upload" copyrighted content to their own servers, thereby making an unauthorized reproduction. Whether a site would be found directly or secondarily liability depends on the facts of how unauthorized copies are made and how much interaction the site has with the process of making them. In the case of a site that "hosts" copyrighted content on its own servers that users submit to the site, and where the site itself has no interaction with the copying process apart from storing the content (and being the location from which others copy it), a direct liability claim may be more difficult to prove and secondary infringement claims may be more likely to succeed.[39]

On the other hand, a website may be subject to direct liability where it does not simply engage in automated copying in response to users' commands, but makes additional contributions to the creation of the copy.[40] For example, in a case involving widespread uploading and downloading of copyrighted content through a network of computers called the USENET, the court held that the defendant service operators did enough themselves to be deemed directly liable for infringement.[41] The court said that the defendants were "aware that digital music files were among the most popular articles on their service," took "active measures to create servers dedicated to mp3 files and to increase the retention times of newsgroups containing digital music files," and took "active steps" to "remove access to certain categories of content, and to block certain users."[42]

(2) Right of Distribution

The owner of copyright also has the exclusive right to distribute copies of their work "to the public by sale or other transfer of ownership, or by rental, lease, or lending."[43]

Where users are able to obtain unauthorized copies of copyrighted works through a Predatory Foreign Website—for example, where users download copies directly from the site—the site is likely a direct infringer of the distribution right.[44] Where the Predatory Foreign Website's role is to facilitate or encourage users to obtain copies from other sites, then the Predatory Foreign Website's potential liability is secondary.

Although a Predatory Foreign Website may be directly liable for infringing the distribution right, there is some disagreement in the case law about what proof is required to establish that the distribution right has been infringed in the Internet context. In particular, there is some disagreement whether the plaintiff claiming an infringement of this right must show that a file containing an infringing copy of the copyrighted work has actually been transferred to the party that requested it. This proof issue has significance to proving direct infringement of the distribution right because Predatory Foreign Websites are unlikely to maintain records of the files transferred through their service.

In the Ninth Circuit's original *Napster* decision, the court held that there was a direct infringement of the distribution right by Napster users "who upload files names to the search index for others to copy,"[45] which would indicate that no proof of actual transfer is required. In a later proceeding arising out of the *Napster* litigation, the district court held that a violation of the distribution right

required proof either of (1) an "actual disseminat[ion of] one or more copies of the work to the public" or (2) "offer[ing] to distribute copies of that work to the public for purposes of further distribution, public performance, or public display."[46] Still other district courts have held that making a copyrighted work available for others to download, without proof of an actual download, is not sufficient to violate the distribution right.[47] It should be noted that, to the extent that proof of an actual download is required, a copyright owner may be able to establish such a download by showing that investigators retained by plaintiffs for these purposes completed downloads of copyrighted content through the use of a particular website or Internet service.[48]

(3) Right of Public Performance

The owner of copyright in an audiovisual work also has the exclusive right to perform that work publicly. The owner of copyright in a sound recording has the exclusive right to perform that work publicly and perform that work by means of a digital audio transmission.[49]

The Copyright Act defines what a public performance is in two clauses in Section 101 of Title 17. Under clause (1), the "public place" clause, a performance is public if it occurs "at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered."[50] Under clause (2), the "transmit" clause, a performance is public if someone "transmit[s] or otherwise communicate[s] a performance … of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance … receive it in the same place or in separate places and at the same time or at different times."[51]

Numerous cases have held that transmitting performances of the same copyrighted work to members of the public is a public performance, even if the individual members of the public receive the performance in private and at separate times.[52] Where a Predatory Foreign Website is involved in transmitting Internet streams of copyrighted works to multiple users, the site likely is directly violating the public performance right.[53]

b) Secondary Liability of Predatory Foreign Websites—Copyright Law

Even if a Predatory Foreign Website were not itself directly liable for infringements occurring through that site, the site likely would be subject to one or more forms of secondary liability for its active role in promoting and facilitating the infringements of others, most notably the site's users. Copyright law has long recognized that parties may be liable for their role in direct infringements committed by others.[54] Secondary liability has been particularly important in the context of infringement occurring through Internet sites. The Supreme Court in *Grokster* summarized the rationale for secondary liability for infringements occurring through Internet sites: "When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement."[55]

In order to prove a claim for secondary liability, the plaintiff-copyright owner must prove (1) underlying direct infringement(s),[56] and (2) a basis for holding the defendant secondarily liable for the infringement(s). We discuss the established bases for asserting a claim of secondary liability, and issues that may be raised in their application to Predatory Foreign Websites, in the sections that follow.

(1) Contributory Infringement

A party may be liable for contributory infringement where, (1) with knowledge of another's infringing conduct, (2) that party materially contributes to the infringement.[57]

Knowledge. The "knowledge requirement for contributory copyright infringement" includes "both those with *actual knowledge* and those who *have reason to know* of direct infringement."[58]

Where the operator of a website actually knows of specific infringements occurring through the site, then the knowledge prong will be satisfied.[59] If it cannot be shown that the website's operator has actual knowledge of specific infringements, it still may be possible to impute to the operator knowledge of the infringing activity. In particular, if the operator has "willfully blinded" itself to infringing activity taking place through its site, the operator will be deemed to have actionable knowledge.[60]

Where a copyright owner seeks to impute the website's operator knowledge "*solely* because the design [of the website service] facilitates … infringement[,]" the operator may assert as a defense that a website is capable of "substantial noninfringing uses."[61] This defense provides that, where a product or service is "capable of commercially significant noninfringing uses," then knowledge may not be imputed based solely on the service's design.[62] If the copyright owner does not base his or her claim of knowledge exclusively on the service's design, then the "substantial noninfringing uses" defense will not immunize the site's operator from contributory infringement liability.[63]

Copyright owners should be able to show a Predatory Foreign Website's knowledge of infringement in several ways. Depending on the facts, a copyright owner may be able to show that those who operate the site have actual knowledge of infringements taking place through the site. A copyright owner could also provide the site with notices of specific infringing copies of works available through that site, although the task of compiling and sending such notices can be burdensome and frequently may be futile (since additional copies of the same works can and usually do replace the copies that are the subject of the notices). If the operators of the site were to disclaim knowledge of infringement, the copyright owner might be able to show that the operators took active steps to ensure they would not acquire knowledge of specific infringements.

Material Contribution. A service that provides the "sites and facilities" for third parties to engage in direct infringement materially contributes to that infringement.[64] Moreover, the Ninth Circuit has held that "a computer system operator can be held contributorily liable if," in addition to the actual knowledge requirement being satisfied, the operator of that system "can take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works."[65] A service can take "simple measures" to reduce infringement if "there are reasonable and feasible means for [the service] to refrain from providing access to infringing [content]."[66]

It seems likely that a website that provides the site and facilities for users to obtain unauthorized copies of copyrighted works or access to unauthorized performances of works would be deemed to materially contribute to the infringing conduct.

(2) Inducing Infringement

In *Grokster*, the Supreme Court held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for…infringement by third parties."[67] The Court did not establish a bright-line test for what is required to show that a website intends to induce infringement. The Court said that the evidence of defendants' unlawful objective in that case was "unmistakable," given evidence that they "aim[ed] to satisfy a known source of demand for copyright infringement"; failed to "attempt[] to develop filtering tools or other mechanisms to diminish the infringing activity using their software"; and operated a business whose "commercial sense ... turn[ed] on high volume use, which the record shows is infringing."[68]

In cases following the Supreme Court's *Grokster* decision, inducement liability has been found were websites are aware of substantial infringements being committed by users; take steps to attract, retain and assist such users, including through optimizing the service for infringing activity; that depend on high-volume infringing use for the success of the site's business (for example, by increasing user base and associated advertising revenue); and that fail to take steps to mitigate infringing activities.[69]

In the case of many Predatory Foreign Websites, copyright owners likely would have very good claims for inducing infringement. Any analysis would depend on the specific facts concerning particular sites. However, it seems likely that if a site is engaged in large-scale piracy of copyrighted content, that site will feature many of the indicia of intent to induce infringement that *Grokster* and the cases following it have held to be sufficient to establish inducement liability.

(3) Vicarious Liability

A party infringes vicariously by receiving a financial benefit from direct infringement while declining to exercise a right and ability to stop or limit it.[70]

Financial Benefit. The financial benefit prong of the vicarious liability test focuses on whether the defendant receives some form of financial benefit directly attributable to infringing conduct occurring on their sites. "Financial benefit" has been interpreted broadly by the Supreme Court, and has been held satisfied where infringing conduct serves as a lure to increase the user base and associated value of a site, including the potential to realize increased advertising revenues from larger numbers of users.[71]

Under this test, it is likely that a Predatory Foreign Website that uses unauthorized copyrighted material as a lure to the site satisfies the financial benefit standard.

Right and Ability to Control Infringing Conduct. The right and ability prong of the vicarious liability test generally asks whether the defendant "has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so."[72]

Courts have found the test satisfied where the defendant has the legal right to terminate an infringing party's access to the facilities used for infringement.[73] "To escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability."[74] In the case involving the Lime Wire peer-to-peer service, for example, the court found the defendant service and its owner liable where the service "had the right and ability to limit the use of its product for infringing purposes, including by (1) implementing filtering; (2) denying access; and (3) supervising and regulating users."

To the extent that Predatory Foreign Websites maintain the ability to supervise user conduct or terminate users for violating the terms of the site's service, the site likely would be found to have the right and ability to stop or limit infringing activity taking place through the service.

2. Potential Liability of Intermediaries—Copyright

a) Direct Liability of Intermediaries—Copyright

Various types of intermediaries—including ISPs, web hosting services, and search engines—have facilities and services that play an important role in acts of direct infringement by others, especially on the Internet. Current law, however, generally precludes holding such intermediaries liable for direct infringement.

ISPs and web hosting services play a direct role in the distribution of copyrighted content, the reproduction of copies on their servers (in the ISP context, such copies are likely transient, or "cache," copies), and the public performance and display of such content. The case law regarding the "volitional" conduct requirement, discussed in footnote 88, generally precludes a theory of direct infringement, at least as to reproduction and distribution claims in which end users, and not the intermediaries, initiate the process of copying and transferring files.[75]

Various types of services may provide links to infringing content (along with links to non-infringing content), and may "frame" the display or playback of such content on their own sites. These services thus may play an important role in the unauthorized performance or display of content. However, in a significant decision regarding such links and displays, the Ninth Circuit held that search engine services were not subject to direct liability in these circumstances. The court held that, while a "search engine communicates HTML instructions that tell a user's browser where to find" infringing content, it "does not itself distribute copies of the infringing [content]." Rather, the court held, it is the infringing website's "computer that distributes copies" of the infringing content "by transmitting [it] electronically to the user's computer."[76]

b) Secondary Liability of Intermediaries—Copyright

Many ISP and web hosting service subscribers and search engine users are engaged in the direct infringement by transmitting, uploading, and downloading unauthorized copies of copyright content. Such infringement obviously occurs via the "conduit" services and Internet connectivity offered by ISPs, on the servers provided by web hosting services, and through the Internet links generated by search engines. Other intermediaries, such as advertising networks, provide a source of revenue for infringing websites. This section discusses the potential bases under current law for claims of secondary liability against such intermediaries.

(1) Contributory Infringement

Knowledge. Courts generally have been hesitant to find that an intermediary has actual knowledge of infringement without the provision of notice of specific infringing sites.[77] To the extent intermediaries use technologies to track and analyze user behavior, that may result in them being found to have imputed knowledge of infringing conduct even in the absence of any specific notice.[78] For example, to the extent an intermediary's technology responds to user behavior, and that behavior is infringing conduct, an intermediary may be found to have knowledge of infringement. In *Columbia Pictures Industries, Inc. v. Fung*,[79] the court found knowledge under the DMCA safe harbor provisions where "Defendants designed their website to include lists such as 'Top Searches,' 'Top 20 Movies,' 'Top 20 TV Shows,' and 'Box Office Movies,' and Defendants designed these lists *to automatically update to reflect user activities*. These lists included numerous copyrighted works." *Id.* at *17 (emphasis added).

If notice of specific instances of infringement is provided, courts generally have found that actual knowledge exists.[80] Where the underlying sites at issue are predominantly populated with infringing material, courts have suggested that notice of the general site with a list of infringing works available on that site may be sufficient for notice purposes.[81]

To the extent that the intermediary conducts some sort of pre-approval review before allowing websites to engage in the intermediary's network,[82] such review has been found sufficient to establish knowledge for contributory infringement. In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*,[83] for example, the defendant's "site reviewers review[ed] every site before allowing the sites to utilize the Adult Check system… Although they might not detect every copyright violation, there is evidence that many sites contain disclaimers to the effect, 'we do not hold copyrights for these

works.'"[84] The district court held that the defendant knew or should have known that some of the sites contained infringing content.

Material contribution. Courts generally have held that intermediaries make a material contribution to infringement where their technologies substantially assist users in accessing and downloading infringing content, even where such technologies equally assist in the accessing of non-infringing content. In *Perfect 10 v. Amazon*, for example, the Ninth Circuit held that there was "no dispute that Google substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials. We cannot discount the effect of such a service on copyright owners, even though Google's assistance is available to all websites, not just infringing ones."[85]

The law is less clear whether providing financial support services will be held to materially contribute to infringing conduct. In *Perfect 10, Inc. v. Visa Intern. Service Ass'n*,[86] the Ninth Circuit held that credit card processing services did "not help locate and are not used to distribute the infringing images"; and while the services made "it easier for websites to profit from this infringing activity, the issue here is reproduction, alteration, display and distribution, which can occur without payment. Even if infringing images were not paid for, there would still be infringement."[87] The court emphasized that "infringement could continue on a large scale because other viable funding mechanisms are available."[88]

Simple Measures. Intermediaries also may be found to be able to take "simple measures" to block or limit the infringement to which they materially contribute.[89] For example, ISPs may be able to DNS and IP address block to bar end user access to sites containing infringing content.[90] Web hosting services similarly may be able to take down the infringing sites from their servers. And search engines may be able to block and/or filter the results of infringing sites.[91] U.S. courts have recognized that, although search technologies may have certain automated processes, operators can filter out infringing content.[92] With respect to these technical measures, intermediaries may object on the basis of burden, technical feasibility and/or effectiveness.

(2) Inducement

Where an intermediary's technology appears to be designed and operated in a neutral manner vis-à-vis infringement, and where there is no evidence of affirmative intent to promote infringement, courts have not found inducement liability. For example, in *Perfect 10 v. Amazon*, the Ninth Circuit held that Google's activities did "not meet the 'inducement' test explained in *Grokster* because Google has not promoted the use of its search engine specifically to infringe copyrights."[93] There may be grounds for a copyright owner to raise an inducement claim against some intermediaries where there is affirmative evidence of an intent to induce infringement, however such evidence would be case specific and is not readily apparent in the case of many major commercial intermediaries.

(3) Vicarious Liability

Right and Ability to Stop or Limit Infringing Content. Pursuant to their end user terms of service, ISPs and web hosting sites generally have the right and ability to cut off user access to infringing sites and terminate the accounts of infringing subscribers.

With respect to search engines, the Ninth Circuit has held that the right and ability that counts is the right and ability to stop or limit the infringement effected by the direct infringer—holding with respect to Google and third-party infringing sites that "Google's failure to change its operations to avoid assisting websites to distribute their infringing content may constitute contributory liability

. . . . However, this failure is not the same as declining to exercise a right and ability to make third-party websites stop their direct infringement."[94]

Financial Benefit. As noted above, courts generally have held that a site's expansion of its user base through increased infringing content constitutes a "financial benefit" directly attributable to the infringement. In *Napster*, the Ninth Circuit held that the plaintiffs likely would succeed in establishing that Napster had a direct financial interest in infringing activity given the "[a]mple evidence support[ing] the district court's finding that Napster's future revenue is directly dependent upon 'increases in user base.' More users register with the Napster system as the 'quality and quantity of available music increases.'"[95] More generally, courts have held that a "[f]inancial benefit exists where the availability of infringing material 'acts as a 'draw' for customers,'" and that it need not be a "substantial" draw.[96]

In the context of intermediaries, however, which have substantial non-infringing uses, some courts have rejected general allegations that intermediaries derive a financial benefit from infringement. For example, courts have held with respect to search engines that a plaintiff must establish that the financial benefit at issue is *directly related* to the infringement. In one case, for example, the court rejected the plaintiff's allegation that Google's "advertising revenue is directly related to the number of Google users and that the number of users 'is dependent directly on Google's facilitation of and participation in the alleged infringement.' . . . This vague and conclusory statement does not allege any actual relationship between infringing activity and the number of users and thus does not allege obvious and direct financial interest sufficient to maintain this claim of vicarious infringement."[97]

C. Potential Liability of Predatory Foreign Websites and Intermediaries—Trademark

1. Potential Liability of Predatory Foreign Websites—Trademark

Predatory Foreign Websites that sell counterfeit products and/or which use confusingly similar domain names as a plaintiff's mark may be found directly liable for trademark infringement.

Section 32 of The Lanham Act, 15 U.S.C. §1114, provides liability for trademark infringement if, without the consent of the registrant, a defendant uses "in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark: which is likely to cause confusion, or to cause mistake, or to deceive." Courts routinely find that the selling of counterfeit products on a website that are the same or nearly identical to a trademark owner's genuine product violates Section 1114.[98] Similarly, trademark owners may have a claim for false designation of origin under 15 U.S.C. §1125(a)—*i.e.,* whether the public is likely to be deceived or confused by the similarity of the marks at issue.[99] Further, if the Predatory Foreign Website is using a domain name which is identical or confusingly similar to, or dilutive of, the plaintiff's mark, the plaintiff may have a claim under the Anti-Cybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C. §1125(d).[100]

Given that Predatory Foreign Websites selling counterfeit goods engage in commercial transactions with consumers, courts routinely find that they have purposefully availed themselves of the forum state and are subject to personal jurisdiction.[101] That said, the operators of such sites typically do not subject themselves to the court's jurisdiction, resulting in a default judgment against them. In such situations, so long as the site's domain name is "located" in the United States (*i.e.*, is issued by a U.S.-based registrar or registry), the ACPA allows the owner of a mark to file an *in rem* civil action against a domain name if the domain name violates the owner's trademark rights, and if the owner of the mark satisfies certain procedural provisions.[102] In an *in rem* action, the remedies are limited to forfeiture, cancellation, or transfer of the infringing domain name to the owner of the mark.[103]

2. Potential Liability of Intermediaries—Trademark

a) Direct Liability of Intermediaries—Trademark

Direct liability for trademark counterfeiting against intermediaries such as a search engine, ISP, or web hosting service may be difficult to establish in the absence of evidence that the intermediary "actively participate[d] as a moving force in the decision to engage in the infringing acts or otherwise cause the infringement as a whole to occur."[104] In *Parker v. Google*, the plaintiff alleged that Google's "republication" of a website, which contained defamatory comments about the plaintiff, constituted a Lanham Act violation in that consumers looking for the plaintiff's website and products would find the defamatory and infringing website in their search results and think it was a website produced by the plaintiff. The court granted Google's motion to dismiss this claim, given that there was no allegation that "Google in any way participated in the creation of the website's content or use of his mark. . . . It is clear that Google's 'republication of the [website]' cannot possibly make it a 'moving force' in the infringement."[105] Given that most major ISPs, search engines, and web hosting services have no participation in the decision of Predatory Foreign Websites to engage in trademark infringement, it is unlikely that they could be found directly liable for such infringement.

With respect to advertising networks, there may be a stronger basis for direct liability. In *Rescuecom Corp. v. Google Inc*., the Second Circuit held that Google's policy permitting advertisers to use a plaintiff's marks as keywords in its AdWords program and to use the marks in the text of advertisements constituted Google's "use in commerce" as defined in 15 U.S.C. §1127, as Google "is recommending and selling to its advertisers [the plaintiff's] trademark," "displays, offers, and sells [the plaintiff's] mark to Google's advertising customers when selling its advertising services," and "encourages the purchase of [the plaintiff's] mark through its Keyword Suggestion Tool."[106] The plaintiff still must prove that such use results in a likelihood of consumer confusion.

b) Secondary Liability of Intermediaries—Trademark

Generally, the "tests for secondary trademark infringement," contributory and vicarious infringement, "are even more difficult to satisfy than those required to find secondary copyright infringement."[107]

(1) Contributory Trademark Infringement

Courts have held that "there are two ways in which a defendant [service provider] may become contributorily liable for the infringing conduct of another: first, if the service provider 'intentionally induces another to infringe a trademark,' and second, if the service provider 'continues to supply its [service] to one whom it knows or has reason to know is engaging in trademark infringement.'"[108]

With respect to inducement, courts have held, similar to the copyright context, that there must be evidence of "affirmative acts" made with the intent to induce third parties to infringe a plaintiff's mark. In *Perfect 10, Inc. v. Visa Intern. Service Ass'n*, Perfect 10 alleged that the defendant credit card processing services were "providing critical support to websites that are using the PERFECT 10 mark in a manner that is likely to cause the public to believe that they are authorized by Perfect 10."[109] The Ninth Circuit rejecting this allegation, noting that there was no evidence of "affirmative acts by Defendants suggesting that third parties infringe Perfect 10's mark, much less induce them to do so."[110] As noted above, such evidence would be case specific, but is not readily apparent in the case of many major commercial intermediaries.

With respect to the "knowledge"-based infringement test, courts have held that the knowledge at issue must be specific and not generalized. In *Tiffany (NJ) Inc. v. eBay Inc*., the Second Circuit rejected a contributory trademark infringement claim against an Internet auction site, eBay, by a

trademark owner, Tiffany, whose mark was being used by jewelry counterfeiters on eBay's site.[111] The record at trial in that case contained evidence "demonstrat[ing] that eBay had generalized notice that some portion of the Tiffany goods sold on its website might be counterfeit," having received "thousands of [Notice of Claimed Infringement Forms] [Tiffany] filed with eBay alleging . . . that certain listings were counterfeit."[112] The Second Circuit held that such evidence was insufficient to satisfy the "knows or has reason to know" requirement and that Tiffany "would have to show that eBay knew or had reason to know of specific instances of actual infringement beyond those that it addressed upon learning of them."[113] The Second Circuit noted, however, that had there been evidence of willful blindness, that would have satisfied this standard.[114] "[C]ontributory liability may arise where a defendant is (as was eBay here) made aware that there was infringement on its site but (unlike eBay here) ignored that fact."[115]

Indeed, failure to remove infringing websites in response to notices may result in liability for intermediaries. In *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*,[116] the defendants were U.S.-based web hosting services primarily servicing Chinese customers, some of whom advertised and sold counterfeit goods, including counterfeits of Louis Vuitton, to a U.S. and global consumer base. Louis Vuitton sent copyright and trademark takedown notices to the defendants, some of which they ignored. Louis Vuitton sued for direct and secondary copyright and trademark infringement, alleging that the defendants "had actual knowledge of the websites' activities," "knowingly avoided learning the full extent of the infringing activities and deliberately disregarded Louis Vuitton's notifications," and "knowingly enabled the infringing conduct by hosting the websites and willfully permitting websites to display the products."[117] The case went to trial and the jury returned a verdict for Louis Vuitton, holding the defendants liable for willful contributory infringement of Louis Vuitton's trademarks and copyrights. On appeal, the defendants argued that the court's jury instructions for contributory trademark infringement "failed to distinguish between the servers or services provided by [defendants] and the websites maintained by [defendants'] customers."[118]

The Ninth Circuit rejected this argument, stating that the defendants "physically host websites on their servers and route internet traffic to and from those websites" and defendants "had direct control over the 'master switch' that kept the websites online and available."[119] The Ninth Circuit further rejected the argument that contributory infringement had to be intentional, holding that a plaintiff must only prove that "defendants provided their services with actual or constructive knowledge that the users of their services were engaging in trademark infringement . . . . An express finding of intent is not required."[120]

In *Chloe SAS v. Sawabeh Info. Svcs. Co.*,[121] several luxury brands sued 18 individuals who sold counterfeit versions of the plaintiffs' trademarked goods and a group of foreign-based internet companies that promoted and facilitated the sale of the counterfeit goods through several websites, including www.TradeKey.com. The court found that the sale of counterfeit goods was a large component of TradeKey's business, as evidenced by the "Replica Products" and "Replica Retention" divisions of TradeKey's sales department, and TradeKey keyword reports for fake branded products.[122] According to the decision, the counterfeiting occurred on a large scale, as TradeKey solicited wholesale buyers and distributors worldwide to become paying premium members of TradeKey.com.[123] The court agreed with plaintiffs that they "have established through uncontroverted evidence both the necessary predicate of underlying direct counterfeiting by TradeKey Members, and TradeKey Defendants['] contributory liability for the direct counterfeiting occurring on their website at TradeKey.com."[124] In particular, the court found that (1) TradeKey Members offered for sale counterfeit versions of plaintiffs' trademarked products; and that (2) TradeKey "continued to supply [their] services to one who [they] knew or had reason to know was engaging in trademark infringement;" and (3) TradeKey "had '[d]irect control and monitoring of the instru-

mentality used by a third party to infringe' [Plaintiffs'] marks."[125] Therefore, the court held the TradeKey defendants contributorily liable for counterfeiting and trademark infringement.

(2) Vicarious Trademark Infringement

Vicarious liability for trademark infringement requires "'a finding that the defendant and the infringer have an apparent or actual partnership, have authority to bind one another in transactions with third parties or exercise joint ownership or control over the infringing product.'"[126]

As courts have held, the control must be with respect to the infringing *product*. In *Rosetta Stone*, the Fourth Circuit held that evidence that "Google jointly controls the appearance of the ads or sponsored links on Google's search-engine results page" is "not evidence, however, that Google acts jointly with any of the advertisers to control the counterfeit ROSETTA STONE products."[127]

Furthermore, as the Ninth Circuit held in *Perfect 10, Inc. v. Visa Intern. Service Ass'n*, enabling a transaction for an infringing product likewise is insufficient to satisfy the vicarious standard. There, the plaintiffs argued that the defendants and the infringing websites were "in a symbiotic financial partnership pursuant to which the websites operate their businesses according to defendants' rules and regulations and defendants share the profits, transaction by transaction."[128] The Ninth Circuit held that there was no evidence of vicarious infringement, stating that "Defendants process payments to these websites and collect their usual processing fees, nothing more."[129]

As with the inducement context, evidence satisfying the vicarious standard is not readily apparent for many major commercial intermediaries.

D. Practical and Legal Challenges to Suing Predatory Foreign Websites

There are practical and legal obstacles to bringing actions against the operators of Predatory Foreign Websites.

First, Predatory Foreign Websites are typically hosted on servers located overseas and their operators may go to great lengths to mask their identities,[130] making it hard for copyright and trademark owners to track down and bring claims against them. As the Registrar of Copyrights noted in recent testimony before the House Committee on the Judiciary, "unlike traditional brick-and-mortar infringers, rogue website operators can be extremely difficult to identify or locate, especially if they are based outside the United States. As a result, pursuing them can be hopelessly frustrating for copyright owners and law enforcement agencies alike . . . ."[131] This concern equally applies in the trademark counterfeiting context.

Moreover, even if the location and identity of a Predatory Foreign Website operator could be determined, there are legal challenges to filing suit against them in the U.S. It may be difficult, for example, to establish personal jurisdiction over the site. Courts have held that the "'sheer availability' of allegedly infringing video files" on a foreign website is "insufficient to support [personal] jurisdiction" where the "files were uploaded by unsolicited" users "acting unilaterally and were equally available to all other . . . users regardless of their location."[132]

Where personal jurisdiction has been exercised over foreign sites hosting and distributing infringing content, the sites typically have engaged in some additional conduct targeting the forum state, such as selling advertisements to companies located within the state, promoting the site on state-based websites, or offering paid subscription services to users in the state.[133] And even if a court would find personal jurisdiction to exist over the operator of a Predatory Foreign Website, the operator in all likelihood would not appear in an action in U.S. court and subject itself to jurisdiction, default, and would be beyond the effective reach of any judgment or order the court could issue.

Finally, the alternative of pursuing litigation in the home country of a Predatory Foreign Website can be very costly, time-consuming, and often futile given the absence of law (or judicial inclination to enforce a law) that adequately protects the rights of copyright and trademark owners in the relevant jurisdiction. Indeed, the absence of legal protection for copyright and trademark owners in a particular country is often why the Predatory Foreign Website exists in that country.

E. Injunctive Relief against Intermediaries in Absence of Liability Finding

Given the relative lack of clarity as to whether intermediaries can be held liable for direct or secondary infringement, it is worth considering whether, in the absence of such liability, there is a legal basis to require the intermediary to take some action to stop or limit infringing conduct that its services facilitate. As noted, in cases involving infringement committed directly or abetted by Predatory Foreign Websites, the likelihood is low that any remedial order of judgment in the U.S. will be effective against the site.

There are some bases under existing law whereby a court may have authority to order intermediaries to take some remedial action, even if those intermediaries are not themselves subject to infringement liability.

First, with respect to copyright, the text of the provision authorizing injunctive relief for copyright violations is broadly worded and does not limit injunctive relief to parties found liable for infringement. The statute provides that courts may "grant temporary and final injunctions on such terms *as it may deem reasonable to prevent or restrain infringement of a copyright*."[134] While the text of the statute thus may support the issuance of some form of injunction against a non-liable third party, the decisional authority on this issue suggests that a party that is not liable for infringement is not subject to the court's equitable powers.[135]

Second, there is authority (outside of the context of intellectual property disputes) for the general proposition that a court may have authority to issue injunctions against parties who themselves are not liable, provided that the injunctive measures are "necessary to grant complete relief" and their effect on the non-liable party would be "minor and ancillary."[136]

Third, as noted, some courts have considered the propriety of injunctions against third-party domain name registries in cybersquatting and trademark cases. In *Chanel, Inc. v. Lin*,[137] Chanel sued to shut down various websites. The district court granted Chanel's request that non-party top-level domain registries be required to remove the domains at issue from the Internet. The court noted that although it had "expressed concern" over whether "it was appropriate to issue such an order against a third party," it was "persuaded that this remedy is authorized under 15 U.S.C. §116 and necessary to effectuate the purposes of the injunction in this case."[138] And at least two courts have issued injunctions in the cybersquatting and trademark context ordering several non-party search engines and social media sites to de-index hundreds of infringing sites from their engines.[139] These orders appear to be form default orders submitted by the parties. It is unclear whether the various intermediaries listed as subject to the injunctive provisions have complied with these orders.

No court has yet considered this line of cases in the context of copyright infringement and intermediaries. As discussed above with respect to contributory infringement and "simple measures," a case can be made that ISPs blocking DNS or IP addresses of infringing sites or search engines de-indexing search results is both "minor and ancillary," and necessary to obtain "complete relief" in the absence of any meaningful relief against the underlying infringing site itself.

F. Proposed Civil Remedies and their Application to Predatory Foreign Websites and Intermediaries

The resolution supported by this chapter of the White Paper does not seek to enlarge or diminish any existing remedy against domestic infringers provided by current U.S. law, with respect to conduct already governed by the Copyright Act (17 U.S.C. §101 *et seq.*) or the Trademark Act (15 U.S.C. §1051 *et seq.*). Rather, this White Paper seeks to extend existing remedies available today to redress online piracy and counterfeiting by domestic websites to redress online piracy and counterfeiting by Predatory Foreign Websites. Some of the existing remedies are not particularly suited to the online environment, and their limitations will be discussed below.

The proposed civil remedies focus on three groups: Predatory Foreign Websites, intermediaries (foreign or domestic), and U.S.-based consumers.

1. Remedies Directed to Predatory Foreign Websites

a) Injunctive Remedies

Under current law, a court has the authority to issue three types of injunctive remedies: temporary restraining orders, preliminary injunctions, and permanent injunctions. Fed. R. Civ. P. 65.

(1) Temporary Restraining Orders

Temporary restraining orders ("TROs") serve as a short-term measure, providing immediate relief against a party's continued activity. They are used while a court considers a motion for a preliminary injunction. TROs may be granted on an *ex parte* basis, without knowledge or notice beforehand to the defendant. Fed. R. Civ. P. 65(b)(1).[140]

Several courts use a four-part balancing test to decide whether a TRO is justified:

1. likelihood of success on the merits;
2. the extent of irreparable harm to the plaintiff by the defendant's conduct;
3. the extent of irreparable harm to the defendant if the TRO issues; and
4. the public interest.[141]

At present, plaintiffs seeking remedies against foreign infringing sites have sought temporary restraining orders at the outset of their cases. For example, in *True Religion v. Xiaokang Lei*, [142] the plaintiff obtained a TRO that:

- restrained defendants and any third parties acting in concert with them from selling allegedly infringing items;
- enabled broad financial discovery and discovery from third-party service providers (MasterCard, Visa, PayPal, registrars, advertising services);
- third-party financial providers were ordered to freeze defendants' funds; and
- domain name registrars were ordered to temporarily disable domain names.

Some commentators have argued that there are more than the usual number of due process concerns[143] associated with disabling foreign websites, however temporarily, through the execution of an *ex parte* TRO. Most of these stated concerns center on the lack of adversarial proceedings prior to a website being disabled.[144] Under current U.S. law, however, due process rights are protected even in *ex parte* proceedings. The IPL Section encourages legislators to use existing legislative models (for instance Federal Rule of Civil Procedure 65) as a basis for maintaining protection of due process rights of the defendants in these cases.

Legislative revisions to provide standardized processes to enforce U.S. rightsholders' rights against Predatory Foreign Websites and to ensure that due process concerns of the website owners and/or applicable intermediaries are taken into consideration would ensure the consistent application of available remedies.

(2) Preliminary Injunctions

After a TRO expires, it is succeeded by a preliminary injunction, often covering the same grounds, providing relief to the plaintiff during the duration of the lawsuit, until final judgment is entered.[145] A preliminary injunction may issue only on notice to the adverse party.[146]

As with a TRO, a balancing test of four elements is used to decide whether to grant a preliminary injunction:

1. likelihood of success on the merits;
2. the extent of irreparable harm in the absence of preliminary relief;
3. the balance of equities weighing in favor of the party seeking the injunction; and
4. the public interest.[147]

Cases against Predatory Foreign Websites may involve preliminary injunctions. For example, in *Philip Morris,* the court entered a preliminary injunction:[148]

- prohibiting defendants from using any Philip Morris marks in websites, domain names, links, or search engines or selling Philip Morris products;
- directing the top-level domain registry to transfer the subject domain names to a new registrar, GoDaddy;
- ordering GoDaddy to change the DNS records for the domain names to point to a notice service website hosting the case documents; and
- directing Western Union to "divert" and hold all money transfers sent by U.S. consumers to three named individuals in China.

(3) Permanent Injunctions

Permanent injunctions are granted as final relief, at the end of litigation, after both sides have been afforded the opportunity to be heard. These injunctions may be awarded if a party can demonstrate:

(1) that it has suffered an irreparable injury;

(2) that remedies available at law are inadequate to compensate for that injury;

(3) that considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and

(4) that the public interest would not be disserved by a permanent injunction. [149]

Moreover, "[t]he decision to grant or deny such relief is an act of equitable discretion by the district court, reviewable on appeal for abuse of discretion."[150]

Permanent injunctions remain in effect as long as their necessary conditions are met. Failing to adhere to permanent injunction places a party in contempt of court.[151] In another *Chanel* decision, the court's preliminary injunction:[152]

- prohibited the defendants from using any Chanel marks or selling Chanel products;
- ordered the Defendants' domain names transferred to the Plaintiffs;

- required Google, Bing, Yahoo!, web hosts, domain-name registrars, and domain-name registries that have notice of the Permanent Injunction to "cease facilitating access to any or all websites through which Defendants engage in the sale of counterfeit and infringing goods".

b) Monetary Damages

(1) Difficulties In Collecting Money Damage Awards

Trademark owners can seek damages from counterfeiting foreign websites, including both compensatory and punitive damages, as well as, in some cases, attorney's fees.[153] Unfortunately, enforcing damage awards against foreign website operators is difficult.[154] Some courts have resorted to freezing funds in financial providers such as PayPal.[155]

Copyright owners can seek damages from Predatory Foreign Websites, but these damages may be nearly impossible to collect. Statutory damages are available for copyright infringement, in amounts up to $150,000 per work in the case of willful infringement, or between $750 and $30,000 per work otherwise (subject to what the court deems just).[156] For trademark counterfeiting, the trademark owner is entitled to recover between $500 and $100,000 per counterfeit mark per type of goods of services, or for willful trademark counterfeiting, up to $1,000,000 per counterfeit mark per type of goods or services sold (subject to what the court considers just).[157] Unfortunately, as discussed above, it is next to impossible to collect damages from Predatory Foreign Websites outside of U.S. jurisdiction.

As in trademark counterfeiting actions, funds can be recovered from frozen financial provider accounts (*e.g.*, PayPal). But, for the most part, judgments against Predatory Foreign Websites that U.S. rightsholders might seek to enforce outside of the U.S. would largely be ineffective, unless the country in which the Predatory Foreign Website resides is a party to treaty obligations that require that country's government to "assist" in executing such a judgment. In short, damages sought directly from the Predatory Foreign Website is not currently an effective means to obtain reimbursement for damages suffered in the U.S., although any assets owned in the U.S. by the Predatory Foreign Website might be subject to seizure under certain circumstances.

(2) Domestic Asset Seizure

Trademark and copyright owners can seize domestic-based assets of counterfeiting and pirate websites,[158] but there is a risk that the relevant bank may not comply with the seizure order if the site does not originate in the U.S.[159]

Court orders involving seizures of assets in PayPal accounts have been successful in several recent cases.[160] For instance, in *True Religion*, funds in 84 different PayPal accounts were frozen after plaintiff proved that demonstrated that it was suffering irreparable harm by defendants' counterfeiting and was likely to succeed on the merits of its claims.[161] Similarly, in *Hermès*, the court ordered that PayPal freeze the accounts associated with Predatory Foreign Websites held by unknown owners after plaintiff demonstrated that it was suffering irreparable harm by defendants' counterfeiting and was likely to succeed on the merits of its claims.[162]

2. Remedies Directed to Intermediaries

Because it is so difficult to enforce U.S. court orders directly against foreign Predatory Foreign Websites, a better approach is to focus on their U.S.-based intermediaries. These intermediaries may be served with court orders and compelled to cease providing support services to these websites.

Most intermediaries are for-profit businesses with their own profit motives. Upon receiving a court order, they are induced to take action to reduce their exposure. More often than not, that will mean compliance with the order, if compliance is feasible and if non-compliance carries the risk of being held in contempt of court or incurring a fine.

Making domestic intermediaries subject to court orders against Predatory Foreign Websites carries a concomitant risk to their business interests. Legitimate foreign-based websites, seeking to minimize business risk, could turn away from domestic intermediaries and toward foreign intermediaries, knowing that foreign intermediaries cannot be compelled by U.S. court order. Moreover, it is unlikely that intermediaries will undergo rigorous due-process analysis to protect the rights of defendants—that costs time and money. Thus, safeguards need to be engineered into any legislation to ensure that due process is accorded to foreign website operators.

a) Summary of Cases Involving Court Orders Compelling Intermediaries

Absent specific guidance from Congress about remedies for online piracy and counterfeiting, courts have crafted individualized remedies to address each litigant's individual sets of facts. Some of these have required various intermediaries (as indicated in the table below) to undertake specific obligations:[163]

Case	Fin. Prov.	Advert.	Search Engines	DNS. Reg	Website Hosts	ISPs	Shippers and Carriers
Hermès	✓	✓	✓	✓	✓	✓	✓
Philip Morris	✓			✓			
True Religion	✓	✓	✓	✓		✓	
Chanel v. Eukuk			✓	✓			
Deckers	✓			✓			

In some instances, these court orders have been issued on an *ex parte* basis, before notice was provided to the defendants.[164]

Because they are issued in response to a specific plaintiff's requests, these court orders are generally narrow in scope and require the intermediaries to provide notice to the overseas website to which it provides services.[165]

b) IPL Section Analysis and Recommendations regarding Court Orders Directed to Various Types of Intermediaries

(1) Financial Providers

As discussed above, court orders have been used to require financial providers to freeze funds obtained by counterfeiting or pirate websites, and indeed, have been used in cases such as *True Religion*, [166] *Philip Morris*,[167] *Deckers*,[168] and *Hermès*.[169] Many financial providers already have robust fraud filtering and detection systems, such as: PayPal,[170] Visa,[171] and MasterCard.[172]

Financial providers have argued that any legislation requiring them to freeze a website's assets based on a determination that the website is a Predatory Foreign Website will place an additional burden on these financial providers, thereby necessarily increasing their cost of doing business with legitimate websites. "Given the large number of IP owners and infringing websites, and the

relatively small number of major payment systems and advertising networks, the service providers' monitor costs could be significant."[173] However, given the infrastructure these financial providers already have in place to deal with online fraud, modifying these programs to extend their reach to the seizure of assets from Predatory Foreign Websites would be a reasonable measure.

Financial providers have argued that they should only be required to take action if they are provided with a court order mandating seizure of assets or freezing of the accounts; they also demand safe harbors to defend then against claims of wrongful interference with Predatory Foreign Websites.[174] Some measure of judicial oversight over this process may be necessary to protect the due process rights of the websites and financial providers. Subject to such oversight, however, the IPL Section supports legislation ensuring the availability of such orders against financial providers to Predatory Foreign Websites.

(2) Advertising Networks

Court orders have been used to prevent advertising services from paying Predatory Foreign Websites or from displaying further ads on them.[175] The IPL Section believes these orders were well taken and accordingly supports legislation ensuring the routine availability of such orders in future cases involving Predatory Foreign Websites.

Predatory Foreign Websites can also sell their own advertisements directly, independent of any advertising network intermediary. In these cases, unless the ad buyers can be reached directly, the only remedy available to civil litigants is to seek to shut off the funds directly through the relevant financial provider.

(3) Search Engines

Search engines (*e.g.,* Google Search, Microsoft Bing) drive traffic to websites—including foreign rogue websites—by listing, in response to search terms, content from such websites in so-called "organic" search results that link to those sites. Many of those same search engines also sell keyword-based ads—"sponsored links"—alongside search results (*e.g.*, Google AdWords, Microsoft adCenter). Rogue websites can purchase ads and have them display when consumers search for a particular set of keywords. As with financial companies and advertiser networks, court orders have been issued requiring search engines to remove sponsored links to counterfeiting or pirate websites, in cases such as *True Religion* and *Hermès*. The IPL Section believes these orders were well taken and accordingly supports legislation ensuring the routine availability of such injunctions in future cases involving Predatory Foreign Websites.

Although no U.S. case has yet ordered a search engine to remove counterfeiting or pirate websites from organic search results, it is only a small further step from the order issued in *True Religion*.[176] Moreover, it appears at least possible that the pending de-indexing action by private rightsholders against search engines under the French law implementation of EUCD Article 8(3) will succeed.[177] On the other hand, a similar provision in the SOPA and PIPA bills was almost as controversial as their site-blocking requirements were. [178]

The IPL Section notes that strong arguments exist both for and against the idea of allowing actions against search engines seeking an order that they de-index Predatory Foreign Websites. On the "for" side, it can be argued that search engines are uniquely positioned both to direct users to pirated content and counterfeit goods emanating from Predatory Foreign Websites, and to deter such users from finding those sites by de-indexing them. Moreover, the act of de-indexing is relatively straightforward and low-cost for the search engine—all it has to do is treat the site as if it had requested not to be included in search results, which all search engines routinely allow.[179] As for potential downsides, de-indexing has been criticized as overharsh because it deprives operators

of foreign sites who believe they are not Predatory Foreign Websites of access to US users.[180] But de-indexing does not remove access to the site in question, since a site can always be found by entering its URL or IP address directly into a browser. Nevertheless, routinely allowing orders seeking de-indexing would be a step beyond the current state of US law and would go beyond a "follow the money" approach to addressing the Predatory Foreign Website problem. For these reasons, the IPL Section was unable to reach consensus in support of legislation allowing such orders.

Other types of orders against search engines are also possible. For example, one could imagine an order requiring a search engine to refuse to return search results for the terms "knockoff" or "fake" followed by the name of a trademarked product. However, as Google's counsel testified before the House Judiciary Committee Subcommittee on Intellectual Property, Competition and the Internet, it is very difficult for search engines to proactively block terms like "knockoff" or "fake" to prevent sites selling counterfeit goods from appearing in search results, because such terms have legitimate uses.[181] The IPL Section agrees that such orders raise a number of complicated issues. As such, the IPL Section is unable to recommend that they be authorized at this time.

(4) DNS Registrars

Court orders could require U.S.-based DNS registrars to revoke the registration of a particular domain name used by a Predatory Foreign Website, or otherwise to deprive the Predatory Foreign Website of the right to operate the registered domain, and to redirect users who visit the domain to a notice that the domain was no longer controlled by the Predatory Foreign Website. This has been done as early as in a TRO, as demonstrated in *Chanel,*[182] *True Religion,*[183] *Philip Morris,*[184] *Deckers*, and *Hermès.*[185] Because the vast majority of users access websites through domain names, not IP addresses, a DNS redirect effectively serves as a "kill switch," taking the entire website offline for most users (except for those accessing directly through IP addresses).[186] There is no way for a DNS redirect to only take down the infringing aspects of a website—it is an all-or-nothing proposition and as such serves as a blunt instrument.[187]

DNS redirects may also introduce vulnerabilities into the Internet security system, thus making them less appealing from a technical perspective.[188]

A distinction must be drawn between generic top-level domains whose registries are maintained by U.S. companies, such as .com, .net, .org, .biz, and foreign country TLDs such as .ru, .se, .cn. Under current law, domain names ending in one of the U.S. top level domains can and have been seized and redirected by court order, even when registered through a foreign registrar.[189]

In the context of criminal counterfeiting and piracy enforcement, Immigrations and Customs Enforcement ("ICE") has taken down myriad websites found to provide substantial pirated content or counterfeit products in the past several years.[190]

As yet, no foreign country TLD has been the subject of a U.S. court order, largely because the authoritative registries for foreign country TLDs are based abroad (and domain name redirects have thus far been based on *in rem* jurisdiction over the U.S.-based primary domain name registrar, which is inapplicable to foreign-based registrars such as those for foreign country TLDs).[191] In contrast, the authoritative registry for .com domains is VeriSign, Inc., a public company based in Virginia.

Although the IPL Section recognizes that some courts have ordered DNS registrars like GoDaddy to use DNS redirects, and does not criticize the issuance of such orders in those cases, because of the many issues associated with such redirects, and because it is not a "follow the money" remedy, this is another case where the IPL Section was unable to reach consensus that this remedy should be routinely available to either private parties or governmental entities.

(5) Website Hosts

Court orders have been used to require a host to terminate services to a hosted website, thereby making a counterfeiting or pirate website unavailable.[192] In contrast to search engines, payment processors and advertising services, website hosting is often a more parochial commercial endeavor. Website hosts are often located abroad, making it difficult to enforce orders against them. But the IPL Section believes that U.S.-based website hosts should be subject to injunctions requiring them to cease hosting Predatory Foreign Websites. Accordingly, the IPL Section supports legislation ensuring the routine availability of such injunctions in future cases involving Predatory Foreign Websites.

(6) Internet Service Providers

Court orders could be issued requiring ISPs to filter or otherwise block particular Internet Protocol ("IP") addresses, thus making a counterfeiting or pirate website inaccessible to users of that particular service provider in a particular geographic area ("blacklisting"[193]).[194]

As of yet, IP address blocking of infringing sites has not occurred in the U.S.[195] However, in the U.K., the High Court ordered the five major British ISPs to blacklist both the IP addresses and Uniform Resource Locators ("URLs," or website addresses) for The Pirate Bay as a result of its online piracy activities.[196] This blacklisting featured the U.K.'s a governmentally mandated filtering system, CleanFeed.[197] The Netherlands also implemented a blockade against The Pirate Bay in January 2012, but an April study indicates the block had no effect on BitTorrent traffic.[198] As indicated above, a number of other EU jurisdictions have also issued site-blocking orders. Moreover, in *True Religion* and *Hermès*, court orders were used to order ISPs, among a laundry list of any and all potential third-party services, to "immediately and permanently cease rendering any services" to defendants, although with uncertain effect.

Both SOPA and PIPA would have allowed the DOJ (though not private plaintiffs) to seek DNS-based site-blocking of foreign rogue sites by ISPs, and this provision came under heavy criticism from the technology sector as potentially causing instability in Internet security.[199] As a result of the public outcry about the anticipated risks created by DNS blocking, Rep. Lamar Smith (R-Tx) ultimately withdrew the DNS blocking provision from SOPA in the Manager's Amendment.[200]

This is another case where the IPL Section was unable to reach consensus that this remedy should be available to either private parties or governmental entities.

(7) Shippers and Carriers

In *Hermès*, a court order required "shippers who receive actual notice of the terms of this Permanent Injunction," to "immediately and permanently cease rendering any services" to defendants.[201] The IPL Section believes *Hermès* was rightly decided and accordingly supports legislation ensuring the routine availability of such injunctions in future cases involving Predatory Foreign Websites.

3. Remedies Directed Against Consumers

Finally, while it is technically possible for trademark and copyright owners to proceed with civil litigation against the consuming public who affirmatively seek out counterfeited products or pirated content or engage in illegal file sharing, campaigns like this have been expensive, do not yield significant financial returns, and can cause a public relations problem for the plaintiff in addressing its consuming public.[202]

For instance, the Recording Industry of America ("RIAA") initiated a campaign several years ago against consumers who engaged in illegal file sharing of copyrighted music.[203] During that time,

the RIAA initiated lawsuits against over 18,000 individual users, most of whom paid a few hundred dollars in settlements to avoid the potential for statutory damages of $150,000 per infringing use.[204] More recently, the RIAA has abandoned its former policy of directly bringing cases against consumers in favor of expanding its focus on educating the consuming public about avoiding piracy.[205]

The Motion Picture Association of America ("MPAA") followed in the RIAA's footsteps with its own set of lawsuits directed against consumers who engaged in the illegal file sharing of copyrighted films and other video,[206] though on a vastly smaller scale. It, too, later abandoned this approach.[207]

Based on the information currently available, the IPL Section does not believe that legislative action directly targeting consumers would prove effective in reducing piracy or counterfeiting at this time. Alternatively, a well-constructed and continuous public outreach campaign to educate the public about piracy and counterfeiting, the negative impacts these activities have on the U.S. economy and ways consumers can be proactive in trying to stop such conduct may have a longer lasting positive impact.[208]

IV. CONCLUSION

In light of the analysis above, the IPL Section supports extending certain civil remedies to redress online piracy and counterfeiting undertaken by foreign-based websites. The IPL Section recommends a "follow the money" approach based around extending injunctive relief and monetary damages as detailed more fully above.

Notes

1. Examples of such sites include thepiratebay.se (which originated in Sweden as thepiratebay.org until February 2012 and still has connections there, but has since expanded to a number of other jurisdictions for various parts of its service), and movie4K.to (whose url is registered in Tonga and whose service is currently hosted in the Virgin Islands).

2. *See, e.g.,* S. Rep. 112-39 at 3-4 (2011) (discussing "rogue Internet sites, which do nothing but traffic in infringing goods") (available at http://www.gpo.gov/fdsys/pkg/CRPT-112srpt39/pdf/CRPT-112srpt39.pdf); *compare with* Sen. Wyden Press Release, Wyden, Moran, Cantwell Introduce IP Protection Bill that Will Not Break the Net (Dec. 17, 2011) (available at http://www.wyden.senate.gov/news/press-releases/wyden-moran-cantwell-introduce-ip-protection-bill-that-will-not-break-the-net) (referring to "rogue websites" without definition).

3. The suggestion to cut off the funding source for Predatory Foreign Websites (*i.e.,* "follow the money") is not new. For instance, during the April 6, 2011 hearing before the House Committee on the Judiciary, Subcommittee on Intellectual Property, Competition and the Internet, several participants explored the possibility of "cutting off the money" to these websites as a means to encourage their demise. *E.g*., Senator Conyers' remarks ("Why don't we just cut off all the money? Why don't we eliminate some of the financial incentives by cutting off funding from customer through the payment processing system, or cut off the funding from some of the advertising networks?"); Kent Walker, Counsel to Google (recommending "cutting off the money to these guys, cutting off the advertising . . . [and] the financial services."); Christine Jones, Counsel to GoDaddy (recommending "follow the money" as a means to combat predatory foreign sites); Hr'g Webcast (Apr. 6, 2011) (available at http://judiciary.house.gov/index.cfm/2011/4/hearing-on-promoting-investment-and-protecting-commerce-online-legitimate-sites-v-parasites-part-ii-0). Note that GoDaddy withdrew its support of PIPA and SOPA in the wake of public pressure. *See* Daniel Nye Griffiths, "GoDaddy Retracts Support for SOPA," *Forbes.com* (Dec. 23, 2011) (available at http://www.forbes.com/sites/danielnyegriffiths/2011/12/23/sopa-go-daddy/).

Google has recently renewed its recommendation to use the money trail as a means to stop the websites engaged in online piracy. Theo Bertram, "Follow the Money to Fight Online Piracy," Google Europe Blog (July 2, 2012)

(available at http://googlepolicyeurope.blogspot.com/2012/07/follow-money-to-fight-online-piracy.html) (citing report from BAE Systems Detica, released on July 2, 2012, available at http://www.baesystemsdetica.com/resources/the-six-business-models-for-copyright-infringement/). However, this post urges government pressure on advertising networks and payment processors to follow self-regulatory codes of conduct and does not explicitly endorse legislation requiring them to do so. *Cf.* Testimony of Katherine Oyama, Copyright Counsel, Google, Inc., before the House of Rep. Committee on the Judiciary (Nov. 16, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Oyama%2011162011.pdf) (supporting "follow the money" *legislation*, not just voluntary best practices). *See also* "How Google Fights Piracy" at 3 (September 2013) (available at https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit?pli=1#!), at 3 ("Rogue sites that specialize in online piracy are commercial ventures, which means the most effective way to combat them is to cut off their money supply. Google is a leader in rooting out and ejecting rogue sites from our advertising and payment services, and is raising standards across the industry."). *But see also* Ellen Seidler, "How Google (Doesn't) Fight Piracy," Vox Indie (September 16, 2013), available at http://voxindie.org/how-google-does-not-fight-piracy (taking issue with the preceding claim).

4. Joe Karaganis, "Meganomics," Media Piracy in Emerging Economies, The American Assembly (Columbia University) (Jan. 24, 2012) (available at http://piracy.ssrc.org/meganomics/). Many pirate sites sell subscriptions that provide subscribers with greater capacity limits and higher bandwidth speeds. Even websites that do not sell advertising or access to pirated content frequently solicit donations to maintain servers. *See, e.g.*, Enigmax, "PayPal, IFPI and Police Collaborate to Strangle Pirate Music Sites," *Torrent Freak* (July 23, 2011) (available at http://torrentfreak.com/paypal-ifpi-and-police-collaborate-to-strangle-pirate-music-sites-110723/).

5. This group comprises sites that do not rely on revenue at all, as well as sites that rely on revenue only from non-U.S. intermediaries.

6. Internet security issues presented by DNS blocking options were raised during the public debates about PIPA and SOPA; some examples are worth noting here. For example, SOPA and PIPA allowed courts to order ISPs to intercept and redirect DNS queries for PFWs. A number of commentators argued that such actions would create multiple security issues, as well as hamper efforts to deploy DNSSEC technology. *See* Ram Mohan, "DNSSEC's Time Is Here, But SOPA Presents Challenges," *Security Week* (Jan. 10, 2012) (available at http://www.securityweek.com/dnssecs-time-here-sopa-presents-challenges); *see also* Paul Rosenzweig, "Online Piracy and Internet Security: Congress Asks the Right Question but Offers the Wrong Answers," *The Heritage Foundation* (Jan. 17, 2012) (available at http://www.heritage.org/research/reports/2012/01/online-piracy-sopa-and-internet-security-pipa-bills-in-congress); Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson, Paul Vixie, "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," *CircleID* (May 2011) (available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf). DNSSEC is a technology that was developed to help protect against attackers intercepting steps in the DNS lookup process by digitally 'signing' data so users can be assured the domain they are directed to after submitting a lookup query is valid. (A detailed description of DNSSEC is available here: http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm.)
Critics of SOPA's and PIPA's DNS blocking provisions argued that when ISPs intercept DNS queries, as SOPA and PIPA would have required, applications would be forced to distinguish between malicious attacks on a DNS query—the very evil that DNSSEC was designed to address—and legitimate ISP filtering pursuant to SOPA and PIPA. *See* U.S. Association of Computing Machinery, "Analysis of PIPA's Impact on DNS and DNSSEC" (available at http://usacm.acm.org/images/documents/DNSDNSSEC-Senate.pdf); Steve Crocker, et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," *CircleID* (May 2011) (available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf); Ram Mohan, "DNSSEC's Time Is Here, But SOPA Presents Challenges," *Security Week,* (Jan. 10, 2012) (available at http://www.securityweek.com/dnssecs-time-here-sopa-presents-challenges). The concern was that this would defeat the entire purpose of DNSSEC and would likely lead to a reliance on legacy DNS, making the Internet less safe than it would be if DNSSEC were deployed without DNS blocking. Ram Mohan, "DNSSEC's Time Is Here, But SOPA Presents Challenges," *Security Week* (Jan. 10, 2012) (available at http://www.securityweek.com/dnssecs-time-here-sopa-presents-challenges). A separate concern was based on the fact that DNS filtering does not remove PFW from the Internet—it merely blocks a user from accessing the sites through a specific DNS server connected with their ISP. *See* Steve Crocker, et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," *CircleID* (May 2011) (available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf). As such, users could simply bypass a filtered DNS server by using a non-filtered server. *Id.* To the extent that the non-filtered server did not

employ DNSSEC, which was thought to be likely, it would expose the user to potential malware attacks and other security threats. *Id*.

It should be noted that the above-mentioned Internet security concerns were not universally shared by Internet engineering experts—some thought the concerns were wrong-headed, misleading or overblown. *See, e.g.,* George Ou, "My DNS Filtering Research before House SOPA Panel," HighTech Forum (Dec. 16, 2011) (available at http://www.hightechforum.org/my-dns-filtering-research-before-house-sopa-panel/); George Ou, "DNS Filtering is Essential to the Operation of the Internet," HighTech Forum (June 24, 2011) (available at http://www.hightechforum.org/dns-filtering-is-essential-to-the-internet/). These experts argued that only the small percentage of websites (*i.e.,* PFWs) and users (*i.e.*, users of PFWs) would be affected by the DNS blocking and redirect provisions of SOPA and PIPA, that Congress need not be overly concerned with self-imposed internet security risks incurred by users of PFWs, and that eliminating the redirect requirement so that ISPs were required only to block access to PFWs (as a late Manager's Amendment to PIPA provided) would virtually eliminate any remaining risk of harm to the DNSSEC system. *Id.* For other arguments responding to criticisms of SOPA/PIPA's site-blocking provisions, *see* Daniel Castro, "PIPA/SOPA: Responding to Critics and Finding a Path Forward", *Information and Technology Foundation* at 5-13 (Dec. 2011) (available at http://www.itif.org/files/2011-pipa-sopa-respond-critics.pdf).

7. *See* note 239 (discussing U.S. copyright law provisions for blocking).

8. The so-called "Article 8(3)" legal regime employed by the member states of the European Union is particularly instructive in this regard. Article 8(3) of the European Union's Copyright Directive (2001/29/EC ["EUCD"]) requires member states to "ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right." European Union Copyright Directive 2001/29/EC, Chapter IV, Article 8(3) (*available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:NOT). Member state implementations of EUCD Article 8(3) have successfully been invoked by private rightsholders to obtain no-fault injunctive relief against ISPs (as well as hosting providers) all over the continent. Specifically, orders requiring ISPs to block access to Predatory Foreign Websites, using various types of blocking, have been obtained against ISPs in Austria, Belgium, Denmark, Greece, Finland, Ireland, the Netherlands and the UK. Information about the EUCD can be found here: http://ec.europa.eu/internal_market/copyright/copyright-infso/index_en.htm.

9. A technical overview is available here: http://www.securityweek.com/dnssecs-time-here-sopa-presents-challenges. *See also* Steve Crocker, et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," *CircleID (*May 2011) (available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf).

10. *See* Lauren Mack, "DNS Filtering to Fight Internet Piracy Violates the First Amendment," *Jurist* (Jan. 2011) (available at http://jurist.org/dateline/2012/01/lauren-mack-DNS-filtering.php).

11. *See, e.g.*, Testimony of Katherine Oyama, Copyright Counsel, Google, Inc., before the House of Rep. Committee on the Judiciary at 2-3 (Nov. 16, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Oyama%2011162011.pdf) . Although Google is on record as opposing mandatory de-indexing by search engines, evidence suggests that it de-listed a notorious pirate streaming site named www.Allostreaming.com and related sites on the French version of its search engine in September 2011, following receipt of an August 2011 complaint and significant supporting evidence from several associations of French rightsholders. *See* Enigmax, "Google, Microsoft, Yahoo, ISPs, All Served With Streaming Site Blocking Demand," *Torrent Freak* (Dec. 1, 2011) (available at http://torrentfreak.com/google-microsoft-yahoo-isps-all-served-with-streaming-site-blocking-demand-111201/). In addition to a number of French ISPs, Google's fellow search engines Yahoo! and Bing received the same complaint and evidence. *Id.* Although not reported in the cited article, it appears that Yahoo! and Bing also subsequently de-indexed the same sites on the French versions of their respective search engines. Most recently, the French court before which the evidence was presented has ruled that all French search engines are required to de-index a total of 16 complained-of sites, including but not limited to www.Allostreaming.com and related websites. A description of the decision is available at http://tech2.in.com/news/web-services/french-court-orders-google-and-others-to-block-16-video-streaming-sites/921936 (Nov. 30, 2013).

12. *See, e.g.,* "Obama Administration Responds to We the People Petitions on SOPA and Online Piracy," *The White House Blog* (Jan. 14, 2012) (available at http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-online-piracy).

13. For instance, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (S. 968, the "PROTECT IP Act of 2011" or "PIPA") described the websites to be addressed by the Bill as "the nondomestic domain name used by an Internet site dedicated to infringing activi-

ties" which "(i) conducts business directed to residents of the United States; and (ii) harms holders of United States intellectual property rights." PIPA §3(b)(1), 112th Cong., 1st Sess. (2011) (Leahy) (described in Section 3, entitled "Enhancing Enforcement Against Rogue Websites Operated And Registered Overseas."); S. Rep. No. 112-39 at 3-4 (2011) (available at http://www.gpo.gov/fdsys/pkg/CRPT-112srpt39/pdf/CRPT-112srpt39.pdf) (discussing "rogue Internet sites, which do nothing but traffic in infringing goods")

14. Immigration and Customs Enforcement ("ICE") shut down the music blog Dajaz1.com for over a year before finally declining to pursue judicial forfeiture. Timothy B. Lee, "ICE admits year-long seizure of music blog was a mistake," *ArsTechnica* (Dec. 8, 2011) (available at http://arstechnica.com/tech-policy/2011/12/ice-admits-months-long-seizure-of-music-blog-was-a-mistake/).

15. A restriction to foreign-*hosted* websites avoids entangling domestic-hosted websites that happen to have vanity foreign domain names (*e.g.*, bit.ly). Foreign-hosted refers to the primary web servers for a website, ignoring any content distribution networks.

16. The IPL Section does not attempt to define what amount of evidence must be provided to support a court's conclusion that a website is a Predatory Foreign Website and had the requisite knowledge of its illegal content. Instead, the IPL Section leaves this determination to the Courts or the legislators to define as they deem appropriate.

17. Online sales of counterfeit *physical* copies of copyrighted works (*e.g.,* books, CDs, DVDs and Blu-ray discs) are the obvious exception.

18. A restriction to foreign-*hosted* websites, avoids entangling domestic-hosted websites that happen to have vanity foreign domain names (*e.g.*, bit.ly). Foreign-hosted refers to the primary web servers for a website, ignoring any content distribution networks.

19. The IPL Section does not attempt to define what amount of evidence must be provided to support a court's conclusion that a website is a Predatory Foreign Website and had the requisite knowledge of its illegal conduct. Instead, the IPL Section leaves this determination to the Courts or Congress to define as they deem appropriate.

20. There are over 15,700 financial institutions within the Visa network alone. Written Testimony of Denise Yee before the Senate Judiciary Committee at 3 (Feb. 16, 2011) (available at http://www.judiciary.senate.gov/pdf/11-2-16%20Yee%20Testimony.pdf).

21. Internet Advertising Bureau and PriceWaterhouseCoopers Joint Press Release, "Internet Advertising Revenues Set First Quarter Record at $8.4 Billion" (June 11, 2012) (available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-061112); *see also* the IAB's full report for 2011, published on April 12, 2012 (available at http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2011.pdf).

22. The IAB's analysis is not restricted to revenues generated solely by U.S. activity. Instead, the underlying survey "includes data concerning online advertising revenues from Web sites, commercial online services, free email providers, and all other companies selling digital advertising." Internet Advertising Bureau and PriceWaterhouseCoopers Joint Press Release, "Internet Advertising Revenues Set First Quarter Record at $8.4 Billion" (June 11, 2012) (available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-061112).

23. IAB's annual report for 2011 at 11 (available at http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2011.pdf).

24. *Id.* at 12. Search-based advertising revenue includes "Fees advertisers pay internet companies to list and/or link their company site domain name to a specific search word or phrase (includes paid search revenues). Search categories include:

> **Paid listings**—text links appear at the top or side of search results for specific keywords. The more a marketer pays, the higher the position it gets. Marketers only pay when a user clicks on the text link;
>
> **Contextual search**—text links appear in an article based on the context of the content, instead of a user-submitted keyword. Payment only occurs when the link is clicked.
>
> **Paid inclusion**—guarantees that a marketer's URL is indexed by a search engine. The listing is determined by the engine's search algorithms.
>
> **Site optimization**—modifies a site to make it easier for search engines to automatically index the site and hopefully result in better placement in results."

Id. at 22.

25. *See* BAE Systems Detica, The Six Business Models for Copyright Infringement (June 27, 2012) (available at http://www.baesystemsdetica.com/uploads/resources/The_six_business_models_for_copyright_infringement1.pdf).

26. "Organic search results are listings on search engine results pages that appear because of their relevance to the search terms, as opposed to their being advertisements." "Organic Search," Wikipedia (available at http://en.wikipedia.org/wiki/Organic_search).

27. Google has defended its treatment of counterfeit goods as follows: "Google also expends great effort to meet the challenge of counterfeit goods. Since June 2010, we have shut down nearly 150,000 accounts for attempting to use sponsored links to advertise counterfeit goods. Most of these were proactive removals, done on our own initiative — we received legitimate complaints about less than one quarter of one per cent of our advertisers. Even more ads were blocked on suspicion of policy violations. Our automated tools analyze thousands of signals to help prevent bad ads from being shown in sponsored links. Last year alone we invested $60 million in efforts to prevent violations of our ad policies." Testimony of Katherine Oyama, Copyright Counsel, Google, Inc., before the House of Rep. Committee on the Judiciary (Nov. 16, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Oyama%2011162011.pdf).

28. *See* "Advertising on Google AdWords: An Overview," Google.com (available at http://support.google.com/adwords/bin/answer.py?hl=en&answer=1704410); *compare with* "bing ads," Bing.com (available at http://advertising.microsoft.com/small-business/bing-yahoo-search).

29. *See, e.g.*, "AdWords Trademark Policy," Google.com(available at http://support.google.com/adwordspolicy/bin/answer.py?hl=en&answer=6118).

30. *See* "Internet Service," Comcast.com (available at http://www.comcast.com/internet-service.html).

31. *See* "High Speed Internet," Verizon.com (available at http://www22.verizon.com/home/highspeedinternet/).

32. "Web hosting service," Wikipedia (available at http://en.wikipedia.org/wiki/Web_hosting_service).

33. *Id.*

34. Robert J. Abalos, "Commercial Trademark Counterfeiting in the United States, the Third World and Beyond: American and International Attempts to Stem the Tide," 5 B.C. Third World L.J. 151 (1985) (available at http://lawdigitalcommons.bc.edu/twlj/vol5/iss2/4/).

35. Enforceable jurisdiction encompasses not only personal jurisdiction over the relevant entity (*e.g.*, the website's operators), but also the ability to enforce a judgment against such entity. *See* Section III.D.

36. Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004).

37. 17 U.S.C. §106(1).

38. *See* UMG Recordings, Inc. v. MP3.Com, Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000) (finding defendant service directly liable for infringing reproduction right by copying tens of thousands of CDs to its central servers).

39. There is a split in authority whether "volitional" conduct is required to show direct infringement. *Compare* CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004) ("to establish *direct* liability under . . . the Act, something more must be shown than mere ownership of a machine used by others to make illegal copies. There must be actual infringing conduct with a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner himself trespassed on the exclusive domain of the copyright owner.") *with* Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 130-33 (2d Cir. 2008) ("*Cablevision*") (the person who actually presses the button to make the recording supplies the necessary element of volition, not the person who manufactures, maintains, or owns the machine). Other courts, however, have either rejected or expressed skepticism whether there is a "volitional" conduct requirement for direct copyright infringement, for which there is strict liability and no intent requirement. *See, e.g.*, Warner Bros. Entertainment Inc. v. WTV Sys., Inc., 824 F. Supp. 2d 1003, 1011 n.7 (C.D. Cal. 2011) ("no Ninth Circuit case has adopted this volitional conduct requirement," and "in light of the fact that copyright infringement is a strict liability offense, the Court is not inclined to adopt a volitional conduct requirement without clear instruction from the Ninth Circuit") (quoting *Arista Records, LLC v. Myxer, Inc.,* No. CV-08-3935-GAF at 25 (C.D. Cal. Apr. 1, 2011) (noting that the Ninth Circuit has "consciously declined" to adopt a volition requirement despite having the opportunity to do so in cases "since *Cartoon Network* and *CoStar Group* were each decided")). Courts that have adopted the volitional conduct requirement for direct liability have made clear that the operator of the automated reproduction service may be liable for secondary infringement. *See Cablevision*, 536 F.3d at 132. Secondary liability claims are discussed below.

40. Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 148 (S.D.N.Y. 2009).

41. *See id.* ("contrary to Defendants' contentions, here their service is not merely a "passive conduit" that facilitates the exchange of content between users who upload infringing content and users who download such content; rather, Defendants actively engaged in the process so as to satisfy the "volitional-conduct" requirement for direct infringement.").

42. *See id.*

43. 17 U.S.C. §106 (3).

44. As with the reproduction right, some cases have held that a defendant must act "volitionally" to violate the distribution right. *See* Religious Tech. Ctr. v. Netcom Online Commc'n Servs, Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995). To the extent volitional conduct is required, the Predatory Foreign Website's liability for direct infringement would turn on the degree of interaction the site had with the process of a user obtaining a copy from the site.

45. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001).

46. *In re* Napster, Inc. Copyright Litig., 377 F. Supp. 2d 796, 805 (N.D. Cal. 2005).

47. *See* London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153 (D. Mass. 2008) (holding that making work available for others to download does not establish violation of the distribution right); Capitol Records, Inc. v. Thomas, 579 F. Supp. 2d 1210 (D. Minn. 2008) (reaching same conclusion in granting motion for new trial). In the 2012 appeal in the *Thomas* case (by then renamed "*Thomas-Rasset*"), the Eighth Circuit held that there was no live case or controversy regarding whether the district court's 2008 new trial ruling was correct; there had since been retrials, including the one on appeal, which the appellate court said did not implicate the "making available" issue. Accordingly, the Eighth Circuit held that it did not have jurisdiction to address this issue. *See* Capitol Records, Inc. v. Thomas-Rasset, 692 F.3d 899, 902 (8th Cir. 2012).

48. *See* Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481, 496 (S.D.N.Y. 2011) (collecting authorities).

49. 17 U.S.C. §106 (6). The scope of the right to publicly perform sound recordings by means of digital audio transmissions is limited to paid subscription services and "interactive services," *i.e.*, those that enable "member[s] of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient." 17 U.S.C. §114(d), (j)(7). *See generally* Arista Records, LLC v. Launch Media, Inc., 578 F.3d 148, 152-57 (2d Cir. 2009) (summarizing history of provision on public performance right for sound recordings). The limitations on the public performance right for sound recordings likely do not affect the liability of Predatory Foreign Websites, because most digital audio transmissions from such sites will be in response to end-user requests for particular recordings.

50. 17 U.S.C. §101.

51. *Id*.

52. *See* Columbia Pictures Industries, Inc. v. Redd Horne, Inc., 749 F.2d 154, 159 (3d Cir. 1984) ("transmission of a performance to members of the public, even in private settings . . . constitutes a public performance. [T]he fact that members of the public view the performance at different times does not alter this legal consequence."); On Command Video Corp. v. Columbia Pictures Industries, 777 F. Supp. 787, 790 (N.D. Cal. 1991) ("the relationship between the transmitter of the performance, On Command, and the audience, hotel guests, is a commercial, 'public' one regardless of where the viewing takes place"); Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc., 192 F. Supp. 2d 321, 332 (D.N.J. 2002) ("Because transmission of the clip previews to individual computers occurs when any member of the public selects an icon that redirects him or her to Video Pipeline's website, from which the video clips are then shown, such actions by Video Pipeline constitute a 'public performance'"); Twentieth Century Fox Film Corp. v. iCraveTV, Nos. 00-121, 120, 2000 WL 255989 at *7 (W.D. Pa. Feb, 8, 2000) (holding that transmissions of TV programs over the Internet violated the plaintiffs' public performance rights "by transmitting (through use of 'streaming' technology) performances of the works to the public by means of the telephone lines and computers that make up the Internet.").

In the *Cablevision* case, the Second Circuit held that the defendant (the operator of a "remote storage digital video recorder" service ("RS-DVR")) did not publicly perform works stored on its RS-DVR servers. The defendant argued that the RS-DVR was like a "set top" DVR, where the storage device was located on the defendant's central server rather than on subscribers' television sets. The subscribers themselves initiated the recording process; a unique copy of a program was made and associated with that user who initiated that process; and playback was performed exclusively from the unique copy to the subscriber who had requested that it be made in the first place. The court held that, in these circumstances, the transmissions of performances of the same works from the RS-DVR to its subscribers were private, not public performances. *Cablevision*, 536 F.3d

121, 134-35 (2d Cir. 2008). The applicability of *Cablevision's* public performance holding to other services is a matter of ongoing litigation. *Compare* Warner Bros. Entm't Inc. v. WTV Sys., Inc., 824 F. Supp. 2d 1003, 1011 n.7 (C.D. Cal. 2011) (holding *Cablevision* was inapposite where the defendant transmitted performances from DVDs at its facilities to Internet subscribers) *with* ABC, Inc. v. Aereo, Inc., 874 F. Supp. 2d 373, (S.D.N.Y. July 11, 2012) *aff'd sub nom* WNET, Thirteen v. Aereo, Inc. 712 F.3d 676 (2d Cir. 2013) (cert. granted by ABC, Inc. v. Aereo, Inc., 134 S.Ct. 896 (2014) (declining to issue preliminary injunction where defendant service captured over-the-air broadcast signals and re-transmitted them over the Internet to subscribers using separate individual copies of the same programming for transmissions to each requesting user).

53. Although, as noted above, some courts have held that "volitional" conduct is required to violate directly the reproduction right, even the cases that have recognized such a requirement have been equivocal whether that requirement applies to the public performance right. The *Cablevision* court said that its holding as to the reproduction right "does not dictate a parallel conclusion that the customer, and not [the service] 'performs' the copyrighted work[,]" because "[t]he definitions that delineate the contours of the reproduction and public performance rights vary in significant ways." *Cablevision*, 536 F.3d at 134.

54. *See, e.g., Aimster*, 334 F.3d 643, 645-46 (7th Cir. 2003); Gershwin Pub'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

55. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 929-30 (2005).

56. *See, e.g.*, Faulkner v. National Geographic Enters. Inc., 409 F.3d 26, 40 (2d Cir. 2005).

57. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001); *Gershwin Pub'g*, 443 F.2d at 1162.

58. Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004).

59. *See Napster*, 239 F.3d at 1021-22, n.6 (citing A&M Records, Inc. v. Napster, 114 F. Supp. 2d 896, 918, 920-21 (N.D. Cal. 2000)) (finding Napster had knowledge where RIAA informed Napster of more than 12,000 infringing tracks available through the Napster service; "[a]though Napster, Inc. purportedly terminated the users offering these files, the songs are still available using the Napster service").

60. *See Aimster*, 334 F.3d at 650 ("Willful blindness is knowledge, in copyright law … as it is in the law generally."). In *Aimster*, the service utilized encryption of files being uploaded and downloaded so the service would not know which specific works were being copied. The Seventh Circuit held that the service and its owner had actual knowledge of the unlawful infringements they were facilitating.

61. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1170 (9th Cir. 2007) *("Perfect 10")*.

62. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 442 (1984); *Grokster*, 545 U.S. at 931-32; *Perfect 10*, 508 F.3d at 1170.

63. *Perfect 10*, 508 F.3d at 1170.

64. *Napster*, 239 F.3d at 1022 ("without the support services defendant provides, [] users could not find and download the music they want with the ease of which defendant boasts.").

65. *Perfect 10*, 508 F.3d at 1172 (quoting Religious Tech. Ctr. v. Netcom Online Commc'n Servs, Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995)). .

66. *Id.* at 1172-73.

67. *Grokster*, 545 U.S. at 919. Some courts have questioned whether "inducement" liability is a separate claim for relief, or a subset of general contributory liability. *See, e.g.,* IO Group, Inc. v. Jordon, 708 F. Supp. 2d 989, 999 (N.D. Cal. 2010) ("Given that *Grokster* explicitly states that 'one infringes contributorily by intentionally inducing' infringement, this Court cannot find that inducement to infringe is a separate claim from contributory infringement."); Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 125, 150 n.17 (S.D.N.Y. 2009) ("several courts recently have expressed doubt as to whether inducement of infringement states a separate claim for relief, or rather whether it is a species of contributory infringement"). For purposes of this discussion, it is not material whether inducement is a particular form of contributory infringement or a separate stand-alone claim.

68. *Grokster*, 545 U.S. at 939-40.

69. *See* Arista Records LLC v. Lime Group LLC, 784 F. Supp. 2d 398, 426-31 (S.D.N.Y. 2011); *A*rista Records, LLC v. Usenet.com, 633 F. Supp. 2d at 151-54; Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 984-92 (C.D. Cal. 2006).

70. *See Grokster*, 545 U.S. at 930; Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963). *See also Hotfile*, *supra* fn. 10.

71. *See, e.g., Grokster*, 545 U.S. at 926 ("As the number of users . . . increases, advertising opportunities become worth more"); *Napster*, 239 F.3d at 1023 ("Ample evidence supports the district court's finding that Napster's future revenue is directly dependent upon 'increases in user-base.'").

72. *Perfect 10*, 508 F.3d at 1173.

73. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262-64 (9th Cir. 1996) (flea market owner had control over vendors selling counterfeit music recordings based on the flea market's contractual "right to terminate vendors for any reason whatsoever and through that right . . . the ability to control the activities of vendors."); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1173-74 (C.D. Cal. 2002) (right and ability test satisfied where defendant had a monitoring program in place, purportedly refused to allow sites to use the system until they complied with polices prohibiting infringement, and "control[led] consumer access" and promoted sites).

74. *Napster*, 239 F.3d at 1023.

75. *See CoStar Group*, 373 F.3d at 550 (no direct liability where ISP "designed and managed as a conduit of information and data"; holding that "in the context of the conduct typically engaged in by an ISP," Copyright Act requires "some aspect of volition and meaningful causation-as distinct from passive ownership and management of an electronic Internet facility"); *Cablevision*, 536 F.3d at 131 (no direct liability for violation of reproduction right where cable service's RS-DVR service copied programs at direction of end-users). As noted, not all courts have explicitly adopted the "volitional" conduct requirement for direct infringement. *See WTV Sys.*, 824 F. Supp. 2d at 1010 n.7.

76. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

77. *See, e.g., Napster*, 239 F.3d at 1021 ("[A]bsent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."); Parker v. Google, Inc., 422 F. Supp. 2d 492, 501 (E.D. Pa. 2006), aff'd 242 Fed. Appx. 833 (3rd Cir. 2007) (holding that plaintiff "fails to allege that Google had requisite knowledge of a third party's infringing activity, a failure that is fatal to this claim"; finding insufficient letter to Google that "merely states that the USENET archives contain links to a website that 'contains several postings of mine for which I have not authorized reproduction' and does not make any mention of specific registered works.").

78. *See* Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 648 (S.D.N.Y. Oct. 25, 2011) ("EMI also established that thousands of MP3tunes users visited those infringing links and sideloaded EMI's copyrighted works into their lockers. Moreover, it is undisputed that MP3tunes kept track of that activity. . . . Thus, there is no genuine dispute that MP3tunes had actual knowledge its users had stored and continued to have access to infringing copies of Plaintiffs' works."); *Usenet.com*, 633 F. Supp. 2d at 148-49 (rejecting "passive conduit" defense where, *inter alia*, defendants were "aware that digital music files were among the most popular articles on their service").

79. No. CV 06-5578, 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009).

80. *See, e.g., Ellison,* 357 F.3d at 1077 (finding that plaintiff emailed AOL about his copyright infringement claim and that AOL, despite its changed email address, should have been on notice of the infringing activity); *Capitol Records, Inc.*, 821 F. Supp. 2d at 648 ("MP3tunes' knowledge of the unauthorized use of infringing sideloaded material is manifest. EMI sent three separate takedown notifications identifying hundreds of specific copyrighted works and the specific links on the Sideload website unlawfully distributing those works."); Vulcan Golf, LLC v. Google Inc., 552 F. Supp. 2d 752, 770 (N.D. Ill. 2008) (in trademark context, refusing to dismiss complaint where complaint "alleges that Google was aware of the allegedly infringing nature of the purportedly deceptive domains" where "notice" provided and "Defendants intentionally and blatantly continue to engage in the Deceptive Domain Scheme and the other illegal action alleged herein....')"). *But see* Costar Group Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, 707 (D. Md. 2001) ("notification did not automatically equate to knowledge for the purpose of assessing liability. *Netcom* stands for the proposition that the bare claim of infringement by a copyright holder does not necessarily give rise to knowledge of an infringement.").

81. *See* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 622 (4th Cir. 2001) (plaintiff alerted the defendant to infringement in sufficient detail for DMCA safe harbor purposes when it "identified two sites created for the sole purpose of publishing ALS Scan's copyrighted works" and "virtually all the images at the two sites were [ALS Scan's] copyrighted material'").

82. For example, some advertising networks have terms of service that define websites to which they will not provide advertisements, including sites that violate copyright laws. Postings on blogs and other Internet commentaries indicate that ad networks do review and reject some applicants. Ad networks may also audit the actual appearance of the ad and ensure that other terms of the agreement have been honored.

83. 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

84. *Id.* at 1169.

85. *Perfect 10*, 508 F.3d at 1172. *See also* Perfect 10, Inc. v. Visa Intern. Service Ass'n, 494 F.3d 788, 797-98 & n.8 (9th Cir. 2007) ("Google's search engine itself assists in the distribution of infringing content to Internet users"; "Because location services lead Internet users directly to infringing images and often display them on the website of the service itself, we find that location services are more important and more essential-indeed, more 'material'" than payment services). *Cf.* Flava Works, Inc. v. Gunter, 689 F.3d 754, 760-762 (7th Cir. 2012) (website embedding video from another site not liable for contributory infringement of public performance right where no "admissible evidence that [videos] actually being accessed via myVidster, rather than via other websites, and if they are not, myVidster is not contributing to their performance"); Newborn v. Yahoo!, Inc., 391 F. Supp. 2d 181, 189 (D.D.C. 2005) (dismissing complaint where "there is not even an allegation that the defendants' activities were anything more than 'the mere operation of the website businesses.'").

86. 494 F.3d 788 (9th Cir. 2007).

87. *Visa Int'l Service Ass'n*, 494 F.3d at 796.

88. *Id.* at 797-98.

89. *See Perfect 10*, 508 F.3d at 1172.

90. Courts in other jurisdictions have ordered ISPs to block certain sites. *See* http://www.dslreports.com/shownews/UK-ISPs-Now-All-Blocking-Pirate-Bay-120017 (UK ISPs ordered to block Pirate Bay site); http://www.theinquirer.net/inquirer/news/2114332/belgian-isps-block-pirate-bay (Belgian ISPs ordered to block Pirate Bay site).

91. *See supra* at n. 55 (citing evidence of de-indexing of certain websites in French versions of Google, Yahoo! and Bing search engines*); see also, e.g.,* Mike Masnick, "Argentinean Celebrities Succeed In Forcing Search Engines To Block Search Results On Their Name," *Techdirt* (Nov. 12, 2008) (available at http://www.techdirt.com/articles/20081112/0215062808.shtml). Apparently, Yahoo and Google have implemented certain measures to comply with an Argentinean order requiring them to filter out various content. *See* Firuzeh Shokooh Valle and Christopher Soghoian, "Adios Diego: Argentine Judges Cleanse the Internet," *OpenNet Initiative Blog* (Nov. 11, 2008) (available at http://opennet.net/blog/2008/11/adi%C3%B3s-diego-argentine-judges-cleanse-internet). Most recently, on Nov. 28, 2013, a French court (Tribunal de Grande Instance) in Paris ordered search engines operating in France to de-index 16 websites found to be infringing of the plaintiffs' copyrights (the same decision also ordered ISPs operating in France to block their subscribers' from accessing the same 16 sites). A description of the decision is available at http://tech2.in.com/news/web-services/french-court-orders-google-and-others-to-block-16-video-streaming-sites/921936 (Nov. 30, 2013). No U.S. court has yet held that blocking or filtering search engine results of infringing sites is a "simple measure." In Perfect 10 v. Amazon, the court held that there were "factual disputes over whether there are reasonable and feasible means for Google to refrain from providing access to infringing images." 508 F.3d at 1172.

92. *See, e.g.,* Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660, 2002 WL 1997918, at *11 (S.D.N.Y. Aug. 29, 2002) ("While there is no evidence that MP3Board could control which links were initially found by its automated procedures, MP3Board could delete links from its database and thus prevent them from being displayed in response to user queries. . . .").

93. *Perfect 10*, 508 F.3d at 1171 n.11.

94. *Id.* at 1175. The court reached a similar conclusion with respect to the vicarious liability claim that Perfect 10 brought against credit card processing services. The court held that those services did not have "any ability to directly control that activity, and the mere ability to withdraw a financial 'carrot' does not create the 'stick' of 'right and ability to control' that vicarious infringement requires." *Visa*, 494 F.3d at 803.

95. *Napster*, 239 F.3d at 1023 (quoting A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 902 (N.D. Cal. 2000)). *See also Cybernet Ventures*, 213 F. Supp. 2d at 1174 ("The more new visitors an infringing site attracts, the more money Cybernet makes.").

96. *Ellison*, 357 F.3d at 1078-79.

97. Parker v. Google, Inc., 422 F. Supp. 2d 492, 500 (E.D. Pa. 2006), aff'd 242 Fed. Appx. 833 (3rd Cir. 2007); *see also* Parker v. Yahoo!, Inc., No. 07-2757, 2008 WL 4410095, at *5 (E.D. Pa. Sept. 25, 2008) ("Parker has not set forth any plausible allegations that either defendant financially benefits from this third-party infringement of Parker's copyrighted works, so as to constitute vicarious copyright infringement.").

98. *See, e.g.,* Chanel, Inc. v. chanel255.org, No. 12–21762–CIV, at 6, 2012 WL 1941598, at *4 (S.D. Fla. May 29, 2012) (finding likelihood of consumer confusion where evidence "show[s] that the goods produced and sold by Defendants are nearly identical to genuine Chanel products, indicate[s] that both Chanel and

Defendants target the same U.S. customers on the Internet, suggest[s] that Defendants intended to benefit from the use of Chanel's brand reputation, and show[s] that consumers viewing Defendants' counterfeit goods post-sale would actually confuse them for real Chanel products").

99. *See* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 780 (1992).

100. *See* Shields v. Zuccarini, 254 F.3d 476, 482 (3d Cir. 2001). However, the Ninth Circuit has recently held that there is no cause of action for "contributory cybersquatting" under the ACPA. *See* Petroliam Nasional Berhad (Petronas) v. GoDaddy, Inc., 737 F.3d 546 (9th Cir. 2013) (finding that the ACPA does not provide for contributory liability because its text does not expressly provide for secondary liability, and because common law secondary liability was not incorporated into the ACPA, which created an entirely new cause of action). Other circuits have not yet weighed in on this question.

101. *See, e.g.,* Gucci Am., Inc. v. Wang Huoqing, No. C–09–05969 JCS, at 10, 2011 WL 31191, at *6 (N.D. Cal. Jan. 3, 2011) report and recommendation adopted sub nom. Gucci Am. v. Wang Huoqing, No. C 09–05969 CRB, 2011 WL 30972 (N.D. Cal. Jan. 5, 2011) (finding purposeful availment in default judgment motion where websites offered and sold counterfeit handbags within the forum); Allstar Marketing Group, LLC, v. Your Store Online, LLC, 666 F. Supp. 2d 1109, 1122 (C.D. Cal. 2009) (holding that the exercise of personal jurisdiction was appropriate because "by operating a highly commercial website through which regular sales of allegedly infringing products are made to customers in [the forum state], [the defendant has] purposefully availed [itself] of the benefits of doing business in this district")).

102. 15 U.S.C. §1125(d)(2)(A).

103. *Id*. §1125(d)(2)(D).

104. Parker v. Google, Inc., 422 F. Supp. 2d 492, 503 (E.D. Pa. 2006).

105. *Id*. at 502-503.

106. 562 F.3d 123, 129 (2d Cir. 2009). *See also* Rosetta Stone Ltd. v. Google, Inc., 676 F.3d 144, 153 (4th Cir. 2012) (assuming for purposes of appeal (as it was not disputed by Google) that this constituted a "use" in commerce).

107. Perfect 10, Inc. v. Visa Intern. Service Ass'n, 494 F.3d 788, 806 (9th Cir. 2007); *see also* Sony Corp. v. Universal City Studios, 464 U.S. 417, 439 n. 19, 104 S.Ct. 774 (1984).

108. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 106 (2d Cir. 2010); *see also Visa*, 494 F.3d at 806; Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 855 (1982).

109. 494 F.3d at 807.

110. *Id*.

111. 600 F.3d 93, 106 (2d Cir. 2010).

112. *Id.*

113. *Id*. at 107.

114. *See id.* at 109.

115. *Id*. at 110 n. 15. In Rosetta Stone Ltd. v. Google, Inc., 676 F.3d 144 (4th Cir. 2012), the Fourth Circuit similarly acknowledged that it is "not enough to have general knowledge that some percentage of the purchasers of a product or service is using it to engage in infringing activities; rather, the defendant must supply its product or service to 'identified individuals' that it knows or has reason to know are engaging in trademark infringement." *Id*. at 163. In that case, there was evidence that Google had received a spreadsheet notifying it of approximately 200 instances of sponsored links advertising counterfeit products. The Fourth Circuit reversed the district court's granting of summary judgment to Google, holding that the district court improperly relied upon the *Tiffany* opinion, which "did not view the evidence through the lens of summary judgment; rather, *Tiffany* involved an appeal of judgment rendered after a lengthy bench trial;" by contrast, the evidence in *Rosetta Stone* was "sufficient to establish a question of fact as to whether Google continued to supply its services to known infringers." *Id*. at 165.

116. 658 F.3d 936 (9th Cir. 2011)

117. *Id.* at 941.

118. *Id*. at 942.

119. *Id*. at 943.

120. *Id*.

121. Chloe SAS v. Sawabeh Info. Svcs. Co., No. 11-4147, slip op. at 1 (C.D. Cal. Oct. 8, 2013) (available at http://www.trademarkandcopyrightlawblog.com/wp-content/uploads/2013/11/Order.pdf).

122. *Id.* at 3.

123. *Id.*

124. *Id.* at 5.

125. *Id.* at 8-9.

126. Perfect 10, Inc. v. Visa Intern. Service Ass'n, 494 F.3d 788, 806 (9th Cir. 2007) (quoting Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1150 (7th Cir. 1992)).

127. *Rosetta Stone,* 676 F.3d at 165.

128. 494 F.3d at 808.

129. *Id.*

130. The operators of the Pirate Bay have even proposed placing their servers on aerial drones to prevent copyright owners from locating them. *See* http://www.popsci.com/technology/article/2012-03/pirate-bay-wants-put-network-nodes-sky-aboard-small-aerial-drones.

131. Written Statement of Maria A. Pallante, Acting Register of Copyrights before the Subcommittee on Intellectual Property, Competition, and the Internet, House Committee on the Judiciary (Mar. 14, 2011) (available at http://www.copyright.gov/docs/regstat031411.html).

132. Capitol Records, LLC v. VideoEgg, Inc., 611 F. Supp. 2d 349, 359 (S.D.N.Y. 2009); *see also* Realuyo v. Villa Abrille, No. 01 Civ. 10158, 2003 WL 21537754, *6 (S.D.N.Y. 2003), *aff'd* 93 Fed. Appx. 297 (2d Cir. 2004) ("sheer availability" of allegedly defamatory article on a website insufficient to support jurisdiction despite registered users of the website located in New York). Similarly, courts have declined to exercise personal jurisdiction over individual users who participated in BitTorrent swarms that resulted in copyrighted works being distributed to computers in the forum, holding that such swarms by themselves are insufficient to confer specific jurisdiction over a defendant. *See, e.g.,* Berlin Media Art v. Does 1–654 v. e.k., No.: 11-03770 (JSC), 2011 U.S. Dist. LEXIS 120257, at *4–8 (N.D. Cal. Oct. 18, 2011); Millennium TGA v. Doe, No. 10 C 5603, 2011 U.S. Dist. LEXIS 110135, at *2–8 (N.D. Ill. Sept. 26, 2011); On The Cheap, LLC v. Does 1–5011, No. C10-4472 BZ, 2011 U.S. Dist. LEXIS 99831, at *14 (N.D. Cal. Sept. 6, 2011); *see also* Citigroup Inc. v. City Holding Co., 97 F. Supp. 2d 549, 565-66 (S.D.N.Y. 2000) (distinguishing three different types of uses of an internet website—passive, active and in-between—and holding that only uses of the latter two types show a sufficient connection to the jurisdiction to subject a defendant to personal jurisdiction).

133. *See, e.g., VideoEgg, Inc*., 611 F. Supp. 2d at 360 (finding personal jurisdiction where defendant "sold advertisements to New York companies and sought to participate in advertising campaigns specifically directed at New York users"); DFSB Kollective Co., Ltd. v. Tran, No. 11–CV–01049, at 3-4, 2011 WL 6730678, at *2-3 (N.D. Cal. Dec. 21, 2011) (finding personal jurisdiction where "websites run by [defendant] allow users to request music, and personally download the information" and defendant "uses California companies Facebook, Twitter, and YouTube to promote the websites he operates, and to allow users access to the pirated copies of the copyrighted music and artwork."); Arista Records, Inc. v. Sakfield Holding Co. S.L., 314 F. Supp. 2d 27, 31-33 (D.D.C. 2004) (holding that personal jurisdiction existed over Spanish operator of website where site "allowed users to register for the service but then receive 25 free music files before the user had to pay for further downloads"; holding that "the download of music files by [defendant] constitutes transacting business in the District" of Columbia and is sufficient to establish personal jurisdiction); International Printer Corp. v. Brother Int'l Corp., No. 2–07–CV–361, at 1, 2008 WL 4280345, at *1 (E.D. Tex. Sept. 9, 2008) (specific personal jurisdiction over foreign defendant based in Netherlands was proper where plaintiff presented evidence that foreign defendant's website allowed "users to download allegedly infringing software in Texas" and defendant actually offered allegedly infringing products for sale at a trade show in Texas).

134. 17 U.S.C. §502(a) (emphasis added).

135. *See* Bryant v. Gordon, 503 F. Supp. 2d 1062, 1065-66 (N.D. Ill. 2007) (holding that "because [the defendant] prevailed on [plaintiff's] claim against him, entry of injunctive relief" against the photographer was "improper. . . . The jury's finding that [plaintiff] failed to prove that [photographer] infringed his copyright is binding on the Court with regard to the request for an injunction."); *cf.* Societe Civile Succession Richard Guino v. Int'l Foundation for Anticancer Drug Discovery, 460 F. Supp. 2d 1105, 1110 (D. Ariz. 2006) (remedy of impoundment under §503 of Copyright Act "applies only to infringers"; followed by *Bryant* court).

136. *See* General Building Contractors Association, Inc. v. Pennsylvania, 458 U.S. 375, 399 (1982) (stating, in a case under 42 U.S.C. §1981, that court may have power to impose on non-liable entities "such minor and ancillary provisions of an injunctive order as the District Court *might find necessary to grant complete relief* to [the plaintiffs]." (emphasis added)); U.S. v. Local 30, 871 F.2d 401, 406-07 (3rd Cir. 1989) (affirming a "district court's authority to subject [a party] to injunctive relief [trusteeship] even though the [party] itself was not liable under either §1962(b) or §1962(c) and was only nominally a defendant in the case," noting that "district court can bind a party to an injunction if that party is a nominal party in the action and has an opportunity to respond

and object to the imposition of the injunction" and that "RICO was intended to provide broad equitable relief under §1964(a).").

137. No. C–09–04996, 2010 WL 2557503 (N.D. Cal. 2010).

138. *Chanel*, No. C–09–04996, at 17, 2010 WL 2557503 at *12. *See also* The North Face Apparel Corp. v. Fujian Sharing Import & Export LTD., Case No. 10 Civ. 1630, Dkt. No. 54 (S.D.N.Y. June 13, 2011) (third party domain name registry found to be in contempt of court for failing to comply with the injunction, because it failed to remove the offending domains).

139. *See* Hermes International v. John Doe, 12-CV-1623(DLC), Dkt. No. 14 (S.D.N.Y. Apr. 30, 2012) (entering default judgment and ordering "Google, Bing, and Yahoo, and any social media websites including, but not limited to, Facebook, Google+, and Twitter" to "de-index and remove from any search results pages" infringing domain names and associated websites); Chanel, Inc. v. The Partnerships et al., Case No. 2:11-CV-01508, Dk. No. 37, Nov. 14, 2011 at ¶ 10 (D. Nev.) (same).

140. Fed. R. Civ. P. 65(b)(1) provides: "The court may issue a temporary restraining order without written or oral notice to the adverse party or its attorney only if: (A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required."

141. Pappan Enters. v. Hardee's Food Sys., 143 F.3d 800, 803 (3d Cir. 1998).

142. True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 8-16 (S.D.N.Y. Nov. 18, 2011) (temporary restraining order).

143. For an analysis of these, *see* Lemley, Levine, and Post, "Don't Break the Internet," 64 *Stan. L. Rev. Online* 34 (2011) (available at http://www.stanfordlawreview.org/online/dont-break-internet).

144. *Id.* Indeed, initial versions of SOPA contained a pre-litigation voluntary process which did not require any TRO application or other court involvement:

> Under SOPA, IP rightsholders could proceed vigilante-style against allegedly offending sites, without any court hearing or any judicial intervention or oversight whatsoever. For example, SOPA established a scheme under which an IP rightsholder need only notify credit card companies of the facts supporting its "good faith belief" that an identified Internet site is "primarily designed or operated for the purpose of" infringement. The recipients of that notice will then have five days to cease doing business with the specified site by taking "technically feasible and reasonable" steps to prevent it "from completing payment transactions" with customers. And all of this occurs based upon a notice delivered by the rightsholder, which no neutral third party has even looked at, let alone adjudicated on the merits.

Id. This voluntary process was deleted in a later Manager's Amendment, meaning that the version of SOPA that was withdrawn no longer contained any process that did not require application to a court. Even following such removal, however, both SOPA and PIPA contemplated the possibility of proceedings that were *ex parte* as to the targeted website.

145. Fed. R. Civ. P. 65(a).

146. Fed. R. Civ. P. 65(a)(1).

147. Winter v. Natural Resources Defense Council, 555 U.S. 7 (2008).

148. Philip Morris USA, Inc. v. Jiang, No. 11-cv-24049, 2011 U.S. Dist. LEXIS 142630, at *9 (S.D. Fla. Dec. 12, 2011) (preliminary injunction).

149. eBay Inc. v. MercExchange, L*.L.C*., 547 U.S. 388, 391 (2006).

150. *Id.*

151. *See, e.g.,* Reebok Int'l v. McLaughlin, 49 F.3d 1387, 1390 (9th Cir. 1995) ("District courts do, and must, have the authority to punish contemptuous violations of their orders."); Chanel, Inc. v. Krispin, Case No. 08-23439, 2010 U.S. Dist. LEXIS 123458, at *13 (S.D. Fla. Oct. 18, 2010) ("Without prejudice to entering additional sanctions to enforce compliance with the Court's Permanent Injunction, the immediate relief that should be entered to remedy Defendants' continued non-compliance should be the entry of a Second Amended Order Holding Defendants in Contempt."); Fed. R. Civ. P. 4.1(b) ("An order committing a person for civil contempt of a decree or injunction issued to enforce federal law may be served and enforced in any district.").

152. Chanel, Inc. v. Krispin, Case No. 08-23439, 2010 U.S. Dist. LEXIS 123458 (S.D. Fla. Oct. 18, 2010).

153. *See, e.g.*, Coach, Inc. v. Brightside Boutique, Cause No. 1:11-CA-20 LY, 2012 U.S. Dist. LEXIS 1464

at *10-*11, *24-*25 (W.D. Tex. Jan. 6, 2012) (recommending award of statutory damages, costs and attorneys' fees).

154. *See* Henry (Litong) Chen, "The Enforcement of Foreign Arbitration Awards in China," *Bloomberg L. Rep.* (2009) (available at http://www.mwe.com/info/pubs/BLR_1109.pdf).

155. Immigrations and Customs Enforcement, "More than $896,000 in proceeds seized from the online sale of counterfeit sports apparel manufactured in China," Press Release (Apr. 10, 2012) (available at http://www.ice.gov/news/releases/1204/120410washingtondc.htm) ("Pursuant to warrants issued by a U.S. district judge, law enforcement officers seized $826,883 in proceeds that had been transferred from PayPal accounts to various bank accounts in China.").

156. 17 U.S.C. §504.

157. 15 U.S.C. §1117(c).

158. *See, e.g.*, Lanham Act §34(d)(5)(B), 15 U.S.C. §1116(d)(5)(B); Coach, Inc. v. Brightside Boutique, Cause No. 1:11-CA-20 LY, 2012 U.S. Dist. LEXIS 1464 at *10-*11, *24-*25 (W.D. Tex. Jan. 6, 2012) (recommending award of statutory damages, costs and attorneys' fees); *compare with* Reebok v. McLaughlin, 49 F.3d 1387 (9th Cir. 1995) (seizure rejected for foreign-based assets).

159. "[B]ut it can be difficult to litigate against uncooperative foreign entities and/or to enforce a judgment abroad." Written Statement of Maria A. Pallante, Acting Register of Copyrights before the Subcommittee on Intellectual Property, Competition, and the Internet, House Committee on the Judiciary (Mar. 14, 2011) (available at http://www.copyright.gov/docs/regstat031411.html).

160. Immigrations and Customs Enforcement, "More than $896,000 in proceeds seized from the online sale of counterfeit sports apparel manufactured in China," Press Release (Apr. 10, 2012) (available at http://www.ice.gov/news/releases/1204/120410washingtondc.htm) ("The individuals conducted sales and processed payments for the counterfeit goods using PayPal accounts and then wired their proceeds to bank accounts held at Chinese banks. Pursuant to warrants issued by a U.S. district judge, law enforcement officers seized $826,883 in proceeds that had been transferred from PayPal accounts to various bank accounts in China. The funds were seized from correspondent, or interbank, accounts held by the Chinese banks in the United States. Pursuant to additional seizure warrants issued by a U.S. magistrate judge, law enforcement officers also seized $69,504 in funds remaining in three PayPal accounts used by the subjects.").

161. True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 10 (S.D.N.Y. Nov. 18, 2011) (temporary restraining order).

162. *See Hermès* Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 6-7 (S.D.N.Y. April 30, 2012) (default judgment and permanent injunction).

163. *See* Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623 (S.D.N.Y., April 30, 2012) (default judgment and permanent injunction) (financial providers, advertisers, search engines, DNS registrars, website hosts, ISPs, shippers and carriers); Philip Morris USA, Inc. v. Jiang, No. 11-cv-24049, 2011 U.S. Dist. LEXIS 142630 (S.D. Fla. Dec. 12, 2011) (preliminary injunction) (financial providers, DNS registrars); True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB) (S.D.N.Y. Dec 2, 2011) (preliminary injunction) (financial providers, advertisers, search engines, DNS registrars, ISPs); Chanel, Inc. v. Eukuk.com, et al., No 2:11-CV-01508-KJD-PAL, 2012 U.S. Dist. LEXIS 38481 (D. Nev. March 20, 2012) (sixth temporary restraining order) (DNS registrars, search engines); Deckers Outdoor Corp v. Doe, No. 11 C 10, 2011 U.S. Dist. LEXIS 119448 (N.D. Ill. Oct 14, 2011) (default judgment) (financial providers, DNS registrars).

164. *See* Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 9 (S.D.N.Y., March 6, 2012) (temporary restraining order); Philip Morris USA, Inc. v. Jiang, No. 11-cv-24049, at 5 (S.D. Fla. Nov. 16, 2011) (temporary restraining order); True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 15 (S.D.N.Y. Nov 18, 2011) (temporary restraining order); all of which featured a TRO against trademark counterfeiting websites.

165. Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 10 (S.D.N.Y., April 30, 2012) (default judgment and permanent injunction) ("Further, upon giving actual notice of such an Order to any search engines … such Internet Search … Websites shall de-index and remove from any search results pages."); Philip Morris USA, Inc. v. Jiang, No. 11-cv-24049, at 8 (S.D. Fla. Nov. 16, 2011) (temporary restraining order) ("Upon receipt of this Order, Western Union … shall divert all money transfers"); True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 14 (S.D.N.Y. Nov 18, 2011) (temporary restraining order) ("VeriSign, Inc., Neustar, Inc., and Public Interest Registry … within three days of receipt of this Order, temporarily disable these domain names").

166. True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 10 (S.D.N.Y. Nov. 18, 2011) (temporary restraining order).

167. Philip Morris USA, Inc. v. Jiang, No. 11-cv-24049, 2011 U.S. Dist. LEXIS 142630, at *9 (S.D. Fla. Dec. 12, 2011) (preliminary injunction).

168. Deckers Outdoor Corp v. Doe, No. 11 C 10, 2011 U.S. Dist. LEXIS 119448, at *15-*19 (ND. Ill. Oct 14, 2011) (default judgment).

169. Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 9-10 (S.D.N.Y., April 30, 2012) (default judgment and permanent injunction).

170. PayPal, "Buyer Protection, Seller Protection" (available at https://cms.paypal.com/cgi-bin/marketingweb?cmd=_render-content&content_ID=security/online_security_center).

171. Visa, "Security Program," (available at http://usa.visa.com/personal/security/visa_security_program/index.html) (relating to fraud provention and identity theft protection).

172. MasterCard, "Fraud Prevention: Arming You with Knowledge" (available at http://www.mastercard.us/merchants/security/fraud-prevention.html).

173. Letter from American Express Company et al. to Sen. Patrick Leahy, Chairman of the Senate Comm. on the Judiciary (May 25, 2011) (available at http://cdt.org/files/NC-Letter_on_PRA_on_Protect_IP_Act-4.pdf).

174. Testimony of Denise Yee, Senior Trademark Counsel, Visa, Inc. before the Senate Judiciary Committee, S. Hr'g 112-47 at 15 (Feb. 16, 2011) (available at http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67443/pdf/CHRG-112shrg67443.pdf) ("And the essential part of the legislation—and I agree with my colleagues here, with Verizon and Go Daddy—is the safe harbor and to make sure that we are not penalized for trying to do the right thing."); *see also* Testimony of Thomas M. Dailey, Vice President and Deputy General Counsel, Verizon, , S. Hr'g 112-47 at 15 (Feb. 16, 2011) (available at http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67443/pdf/CHRG-112shrg67443.pdf) ("Immunity from liability is very important because we do not want to be dealing with lawsuits that might follow from some of the activity that could be required under the law.").

175. Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 9 (S.D.N.Y., April 30, 2012) (default judgment and permanent injunction).; True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 9 (S.D.N.Y. Dec 2, 2011) (preliminary injunction).

176. "ORDERED that, in accordance with 15 U.S.C. §1116(a) and this Court's inherent equitable power to issue provisional remedies ancillary to its authority to provide final equitable relief, any third party providing services in connection with any Defendant and/or Defendants' websites, including without limitation ISPs, back-end service providers, affiliate program providers, web designers, and sponsored search engine or ad-word providers, shall immediately temporarily disable service to any and all Defendants' Infringing Web Sites. . . " *True Religion*, No. 11-cv-8242 at 15.

177. *See* Enigmax, "Google, Microsoft, Yahoo!, ISPS, All Served with Streaming Site Blocking Demand,: *Torrent Freak* (Dec. 1, 2011) (available at https://torrentfreak.com/google-microsoft-yahoo-isps-all-served-with-streaming-site-blocking-demand-111201/).

178. *See* n. 56. Each of SOPA and PIPA permitted a governmental entity—the Department of Justice—to seek de-indexing by search engines of websites found by a U.S. District Court to be foreign rogue sites. But neither bill allowed private plaintiffs to seek such relief.

179. *See, e.g.*, Sean Carlos, "6 methods to control what and how your content appears in search engines," *Antezeta* (Feb. 18, 2007) (available at http://antezeta.com/news/avoid-search-engine-indexing).

180. *See, e.g.,* Ariele McWhinney, "SOPA, PIPA and Search Engine Marketing," *Marketing Mojo* (Jan. 19, 2012) (available at http://blog.search-mojo.com/sopa-pipa-search-engine-marketing/).

181. Testimony of Katherine Oyama, Copyright Counsel, Google, Inc., before the House of Rep. Committee on the Judiciary (Nov. 16, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Oyama%2011162011.pdf).

182. Chanel, Inc. v. Eukuk.com, et al., No 2:11-CV-01508-KJD-PAL, 2012 U.S. Dist. LEXIS 38481, at 12 (D. Nev. March 20, 2012) (sixth temporary restraining order).

183. True Religion v. Xiaokang Lei, No. 11-cv-8242 (HB), at 14, 15 (S.D.N.Y. Nov. 18, 2011) (temporary restraining order).

184. Philip Morris USA, Inc. v. Jiang, No. 11-cv-24049, at 5 (S.D. Fla. Nov. 16, 2011) (temporary restraining order).

185. Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 9 (S.D.N.Y., March 6, 2012) (temporary restraining order).

186. Marshall Brain & Stephanie Crawford, "How Domain Name Servers Work," *HowStuffWorks.com* (available at http://www.howstuffworks.com/dns.htm; accessed July 13, 2012).

187. *Id.*

188. A technical overview is available here: http://www.securityweek.com/dnssecs-time-here-sopa-presents-challenges; *see also* Steve Crocker, et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," *CircleID* (May 2011) (available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf).

189. *E.g.*, United States Olympic Committee v. 2000Olympic.com, No. 1:00-cv-1018-A (E.D. Va. 2000) (*in rem* action against 1,800 foreign domain names under Anti-Cybersquatting Consumer Protection Act, 15 U.S.C.§1125(d)). For example, bodog.com was registered with a Canadian company but seized by U.S. authorities because VeriSign is U.S.-based. *See* David Kravets, "Uncle Sam: If It Ends in .Com, It's .Seizable," (Mar. 6, 2012) (available at http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/); *see also* Mike Masnick, "Homeland Security Seizes Spanish Domain Name That Had Already Been Declared Legal," *TechDirt* (Feb. 1, 2011) (available at http://www.techdirt.com/articles/20110201/10252412910/homeland-security-seizes-spanish-domain-name-that-had-already-been-declared-legal.shtml); Terry Hart, "Rojadirecta Seeks Return of Seized Domain Names," *Copyhype* (July 13, 2011) (available at http://www.copyhype.com/2011/07/rojadirecta-seeks-return-of-seized-domain-names/); Mike Masnick, "US Government Admits It Has Seized Hundreds Of Domains Registered Outside The US," *TechDirt* (Mar. 9, 2011) (available at http://www.techdirt.com/articles/20120309/04064518045/us-government-admits-it-has-seized-hundreds-domains-registered-outside-us.shtml). For a list of .org domains seized by the U.S. government, see http://pir.org/policies/takedown-policy/takedown_notices/.

190. *See*, *e.g.*, Press Release, "Operation In Our Sites protects American online shoppers, cracks down on counterfeiters: ICE-led IPR Center seizes 150 website domains selling counterfeit and pirated merchandise," ICE (Nov. 28, 2011) (available at http://www.ice.gov/news/releases/1111/111128washingtondc.htm).

191. Anticybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C. §1125(d)(2)(A) (1999).

192. Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 10 (S.D.N.Y., April 30, 2012) (default judgment and permanent injunction).

193. "In computing, a blacklist or block list is a basic access control mechanism that allows everyone access, except for the members of the black list (*i.e.* list of denied accesses)." Wikipedia, Blacklist (computing) (available at http://en.wikipedia.org/wiki/Blacklist_(computing)).

194. Testimony of Thomas M. Dailey, Vice President and Deputy General Counsel, Verizon, before the Judiciary Committee, S. Hr'g Tr. 112-47 at 10 (Feb. 16, 2011) (available at http://www.judiciary.senate.gov/pdf/11-2-16%20Adams%20Testimony.pdf) ("First, we appreciate the fact that the Committee has included in the legislation provisions that appropriately limit the bill's impact on Internet service providers, such as not requiring a service provider to modify its network or facilities to comply with a judicial order. Second, we think the limitation that ISPs will be required to take action only pursuant to a judicial order issued in a lawsuit filed by the Department of Justice will help ensure COICA is narrowly invoked.").

195. 17 U.S.C. §512(j) (the DMCA) sets forth conditions under which a court may grant injunctive relief against service providers that are not subject to monetary remedies because they qualify for one or more DMCA "safe harbors". In the case of ISPs, §512(j)(1)(B)(ii) expressly allows issuance of "an order restraining the [ISP] from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States." Although this section might seem to make the site-blocking provisions of COICA, PIPA and SOPA redundant, this is almost certainly not correct. Although §512(j) is largely unlitigated, it seems clear that, unlike the three recent bills, a plaintiff seeking a site-blocking injunction under §512(j) has to first establish that the ISP is *itself* liable for direct or secondary copyright infringement with respect to the "specific, identified, online location outside the United States", *and* the ISP must then establish its eligibility for a "safe harbor" under §512(a) of the DMCA, before a court is permitted to issue a site-blocking injunction under §512(j). By contrast, of course, COICA, PIPA and SOPA provided for "no-fault" injunctions against ISPs, once the liability of the foreign site sought to be blocked was established. In sum, the three recent bills made obtaining a site-blocking injunction against Predatory Foreign Websites far easier than existing law does.

196. Josh Halliday, "Pirate Bay blockade begins with Virgin Media," *The Guardian (UK)* (May 2, 2012) (available at http://www.guardian.co.uk/technology/2012/may/02/pirate-bay-block-virgin-media).

197. Wikipedia, Cleanfeed (content blocking system) (available at http://en.wikipedia.org/wiki/Cleanfeed_%28content_blocking_system%29).

198. TorrentFreak.com, "Censoring the Pirate Bay is Useless, Research Shows" (Apr. 13, 2012) (available at http://torrentfreak.com/censoring-the-pirate-bay-is-useless-research-shows-120413/).

199. David Sohn, "Copyright Bill Advances, But Draws Plenty of Criticism," *CDT* (May 26, 2011)

(available at http://www.cdt.org/blogs/david-sohn/copyright-bill-advances-draws-plenty-criticism); *see also* David Sohn & Mark Stanley, "The Open Internet Fights Back," *CDT* (Jan. 16, 2012) (available at http://cdt.org/blogs/161open-internet-fights-back); Eric Engleman & Chiara Remondini, "Google Plans Home Page Protest Against U.S. Piracy Measures," *Business Week* (Jan. 18, 2012) (available at http://www.businessweek.com/news/2012-01-18/google-plans-home-page-protest-against-u-s-piracy-measures.html); David Lee, "Sopa and Pipa protests not over, says Wikipedia," *BBC News* (Jan. 19, 2012) (available at http://www.bbc.co.uk/news/technology-16628143); "Support wanes in US Congress for anti-piracy bill," *BBC News* (Jan. 19, 2012) (available at http://www.bbc.co.uk/news/world-us-canada-16623831).

200. Press Release, "Smith to Remove DNS Blocking from SOPA" (Jan. 13, 2012) (available at http://judiciary.house.gov/index.cfm/press-releases?ID=1B599847-E075-63F8-612A-C2537551E11B).

201. Hermès Int'l et al. v. John Doe et al., No. 12 Civ. 1623, at 10 (S.D.N.Y., April 30, 2012) (default judgment and permanent injunction).

202. *See also* Mike Masnick, "The Sky is Rising," *TechDirt* (2012) (available at http://www.techdirt.com/skyisrising/).

203. RIAA Press Release, "Recording Industry To Begin Collecting Evidence And Preparing Lawsuits Against File Sharers," RIAA (June 25, 2003) (available at https://www.riaa.org/newsitem.php?content_selector=newsandviews&news_month_filter=6&news_year_filter=2003&id=2B9DA905-4A0D-8439-7EE1-EC9953A22DB9).

204. David Kravetz, "Copyright Lawsuits Plummet in Aftermath of RIAA Campaign," *Threat Level Blog* (May 18, 2010) (available at http://www.wired.com/threatlevel/2010/05/riaa-bump/).

205. *Id.*; *see also* Electronic Frontier Foundation, "RIAA v. The People: Five Years Later" (Sept. 30, 2008) (available at https://www.eff.org/wp/riaa-v-people-five-years-later).

206. Electronic Frontier Foundation, "MPAA v. the People" (available at https://w2.eff.org/IP/P2P/MPAA_v_ThePeople/) (detailing the MPAA's enforcement campaign).

207. Erika Morphy, "A Timely Reminder that MPAA and RIAA Shouldn't Be Trusted with Too Much Enforcement Power." *Forbes* (Jan. 13, 2012) (available at http://www.forbes.com/sites/erikamorphy/2012/01/23/a-timely-reminder-that-mpaa-and-riaa-shouldnt-be-trusted-with-too-much-enforcement-power/2/).

208. Office of the U.S. Intellectual Property Enforcement Coordinator, 2011 IPEC Annual Report on Intellectual Property Enforcement (available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf).

Chapter 3

PRIVATE ENFORCEMENT ACTIONS

I. SECTION POSITION

The IPL Section favors the creation of a private right of action as part of any legislation designed to address Predatory Foreign Websites.

II. SECTION RESOLUTION: TF-07

RESOLVED, the IPL Section supports allowing copyright and trademark rightsholders to pursue civil remedies in order to effectuate the remedies set forth in TF-06 to redress the piracy of their copyrighted works or counterfeiting relating to their trademarks, so that such efforts may supplement civil and criminal efforts that may be undertaken by U.S. governmental actors.

NOW THEREFORE, the IPL Section supports the creation of a private right of action to allow copyright and trademark rightsholders to privately enforce their intellectual property rights against Predatory Foreign Websites as well as the U.S. intermediaries used by such websites, in cases where the intermediaries do not take action voluntarily.

III. DISCUSSION: Private Enforcement Actions

In considering the elements of any future legislation to combat online piracy and counterfeiting emanating from Predatory Foreign Websites, an important consideration is the question of whether or not private enforcement actions should be permitted as a supplement to governmental enforcement actions.[1] Should there be a private right of action by U.S. copyright and trademark rightsholders with respect to such Predatory Foreign Websites, or should the only remedy be an action by U.S. governmental entities? If there is a place for such private rights of action, should they be limited in some way (*e.g.*, with respect to the entities against whom such actions can be brought; with respect to the remedies that can be sought in such actions [*i.e.,* should they be limited to no-fault injunctive relief]; or with respect to a requirement to satisfy pre-conditions before such actions can be brought)?

The IPL Section considers that, as in many other areas of the law,[2] private rights of action with respect to Predatory Foreign Websites serve a valuable function not duplicated by governmental actions and that any future legislation should therefore authorize such actions. Such legislation should allow individual rightsholders to seek the same remedies that the IPL Section recommends be available to governmental actors. The question of whether such intermediaries should be subject to safe harbors or immunity for responding to a rightsholder request that they cease doing business with or on behalf of a Predatory Foreign Website, whether in response to a private action or to voluntary action, is considered elsewhere in this White Paper.

A. Background

The initial legislative proposal addressing rogue websites contemplated only a right of action by the Attorney General, providing private rightsholders with no additional enforcement tools to address their concerns about online piracy and counterfeiting by these Predatory Foreign

Websites.[3] In addition to public comment suggesting that a private right of action might be desirable, several witnesses testified before Congress that allowing a private right of action was necessary in order to allow smaller rightsholders the ability to combat these rogue sites even if the individual violation of their rights was not significant enough to warrant intervention by the government.[4]

B. The Benefits of Allowing Private Rights of Action

As indicated, private rights of action as a supplement—and sometimes even an alternative—to governmental actions are common in many areas of the law, and copyright and trademark law are no exception, both in the US and elsewhere.[5] The usual reason cited for allowing such actions is the increased level of enforcement such actions provide, particularly when governmental resources are scarce, as they almost always are. On a more philosophical level, allowing private parties who are the primary beneficiaries of enforcement of statutory rights to bear the cost of vindicating those rights also arguably aligns costs and benefits associated with the granting of such rights in a way that is superior to the alignment of costs and benefits associated with governmental actions to vindicate the same rights. These benefits have particularly been noted in cases of foreign-based cybercrime.[6] Moreover, private rights of action may actually raise fewer threats to civil liberties than governmental action, particularly with respect to First Amendment and related limitations on governmental power.[7] The private right of action provisions of SOPA and PIPA were heavily criticized when the bills were first introduced,[8] but as time went on, the primary focus of the criticism shifted to their provisions granting immunity from liability to intermediaries for voluntarily complying with the demands of private rightsholders seeking to deny intermediary services to rogue websites. That subject is philosophically distinct from granting rightsholders a private cause of action and is treated elsewhere in this White Paper.[9]

C. Potential Targets for and Limitations on Private Rights of Action

As described in the section of this White Paper on "Remedies,"[10] a private right of action could potentially run against three different groups: Predatory Foreign Websites, intermediaries, and consumers. As that section explains, actions against consumers are problematic in a variety of ways, but actions against PFWs and actions against intermediaries serving such websites are more promising.[11] Recall that under SOPA and PIPA, the private right of action ran only against a rogue site itself (specifically, its registrant, owner/operator(s) and/or its domain name, depending on which of the above could successfully be served), with intermediaries subject to service of any resulting cease and desist order then having a free-standing obligation to cease doing business with the relevant site, subject to a motion to compel in the same court that granted such order.[12] This proposal was subject to criticism from both opponents and supporters of the legislation. Opponents expressed concern that the system encouraged intermediaries, through excessive grants of immunity for complying with such orders, not to object to service of the cease and desist orders, while proponents expressed concern about the lack of judicial economy associated with the prospect of large numbers of drawn-out lawsuits between rightsholders and accused rogue sites, which would threaten to render any subsequent relief from intermediaries too little, too late.

To respond to both criticisms, the IPL Section recommends a hybrid solution, by which rightsholders would be allowed to seek direct remedies directly against PFWs (who would have notice and an opportunity to be heard, including as to any objection to being characterized as a PFW) and direct remedies against one or more of the U.S. intermediaries identified above.[13] This provides full due process rights to the alleged PFW, both in cases where it is sued directly and in cases where its status as a PFW is critical to the issuance of an injunction against one or more of the intermediaries that it uses. Such a procedure is a little less convenient for rightsholders, but it allows the site itself the maximum due process to defend itself against both the onus of being

labeled as a PFW (and resulting liability) and the cutoff of financial support from U.S. intermediaries. Assuming such a procedure in fact strikes the appropriate balance between the rights of rightsholders, the rights of accused PFWs and the rights of the site's intermediaries, the question then becomes whether there should be additional limitations on such private enforcement actions.[14]

D. Limitations on Court Orders against Intermediaries

As noted above, absent guidance from Congress, courts have crafted their own set of court orders compelling intermediaries. Frequently these court orders have proceeded on an *ex parte* basis, often even before notice was provided to defendant parties. The IPL Section also believes that intermediaries subject to these orders should be able to defend against the orders on the basis of burden, technical feasibility and effectiveness, just as they could have had under SOPA and PIPA, as well as under §512(j) of the DMCA, or Article 8(3) in the EU.

Beyond these limitations, the IPL Section believes that the usual rules for civil litigation under the F.R.C.P. should apply, *e.g.*, with respect to each side bearing its own costs and expenses (*i.e.*, no fee-shifting), and with the intermediary bearing any costs associated with compliance with a court's order.[15]

IV. CONCLUSIONS

Based on the analysis explained above, the IPL Section recommends that a private right of action be included in any legislative solution that is proposed in the House or in the Senate to redress online piracy and/or counterfeiting undertaken by PFWs.

Notes

1. Both SOPA and PIPA provided for private rights of action as well as for actions by federal enforcement agencies, albeit not for all of the new causes of action enabled by the bills. *See* §4 of PIPA and §103 of SOPA (each providing for private rights of action with respect to payment processors and advertising networks, but not ISPs and search engines). The predecessor COICA bill, however, provided only for actions by the Department of Justice, a feature that was praised in some congressional testimony. *See, e.g.*, Statement of Thomas M. Dailey, Vice President and Deputy General Counsel, Verizon Communications, Inc. Before the U.S. Senate Committee on the Judiciary, Senate Hr'g 112-47 "Targeting Websites Dedicated to Stealing American Intellectual Property," at 10 (Feb. 16, 2011) ("[W]e think the limitation [in COICA] that ISPs will be required to take action only pursuant to a judicial order issued in a lawsuit filed by the Department of Justice will help ensure COICA is narrowly invoked.") (available at http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67443/pdf/CHRG-112shrg67443.pdf).

2. *See, e.g.*, Section 4(a) of the Clayton Act, 15 U.S.C. §15 (2012) (providing standing for "any person who shall be injured in his business or property by reason of anything forbidden in the antitrust laws" to sue for treble damages); 15 U.S.C.§77k (2012) (providing standing for any purchaser of a security offered pursuant to an initial public offering with respect to which its registration statement contained an untrue statement of a material fact or omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading, to sue for single damages); 18 U.S.C. §1964 (2012) (providing standing to sue for treble damages for "any person injured in his business or property" by reason of anything actionable under the RICO statutes, subject to certain exceptions). The Supreme Court has described Congress' purpose in making such grants of standing as follows: "By offering potential litigants the prospect of a recovery in three times the amount of their damages, Congress encouraged these persons to serve as 'private attorneys general.'" Hawaii v. Standard Oil Co. of California, 405 U.S. 251, 262 (1972) (available at http://supreme.justia.com/cases/federal/us/405/251/case.html).

3. *See* Combating Online Infringements Act ("COICA"), S. 3804, 111th Cong., §2 (2010) (available at http://www.gpo.gov/fdsys/pkg/BILLS-111s3804rs/pdf/BILLS-111s3804rs.pdf).

4. *See, e.g.*, Testimony of Scott Turow, President of the Author's Guild, Before the U.S. Senate Committee on the Judiciary, at S. Hrg. 112-47 "Targeting Websites Dedicated to Stealing American Intellectual Property," at

69 (Feb. 16, 2011) (available at http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67443/pdf/CHRG-112shrg67443.pdf) ("It is critical, above all, to remove two impediments to private causes of action. . . .").

5. *See generally* the Civil Remedies section of this White Paper. Although Italian and Spanish governmental authorities have also obtained site-blocking orders against ISPs in criminal contexts in their respective countries, the overwhelming majority of enforcement activity against intermediaries in Europe has been obtained by private plaintiffs in civil proceedings. *Id.*

6. *See, e.g.,* Michael L. Rustad, "Private Enforcement of Cybercrime on the Electronic Frontier", 11 *S. Cal. Interdisc. L. J.* 63, 66 (2001) (available at http://www-bcf.usc.edu/~idjlaw/PDF/11-1/11-1%20Rustad.pdf,) ("Law enforcement resources in cyberspace cannot keep pace with sophisticated cybercrime subcultures in anonymous offshore havens. As soon as Internet-related criminal statutes are drafted, cybercriminals employ new software tools to attack computer systems. The expanded use of private 'cybercops' and 'private attorneys general,' whose efforts in prosecuting a private suit for an individual client or class of clients also benefits the public, will have to fill the enforcement gap in preventing and punishing wrongdoing on the electronic frontiers.").

7. *See, e.g.,* Mark A. Lemley & Eugene Volokh, "Freedom of Speech and Injunctions in Intellectual Property Cases", 48 *Duke L.J.* 147, 185 & n.176 (1998) (citing New York Times Co. v. United States, 403 U.S. 713, 731 n.1 (1971)).

8. *See, e.g.,* Brian T. Yeh, Congressional Research Service R42112, "Online Copyright Infringement and Counterfeiting: Legislation in the 112th Congress," 23-24 (Jan. 20, 2012) (available at http://www.kelleydrye.com/email/PIPASOPAandtheOPENAct.pdf). Yeh's paper describes two particular concerns that were raised. The first, raised primarily by open internet groups like the Electronic Frontier Foundation (EFF) and the Center for Democracy and Technology (CDT), was that content owners would use the private rights of action provided under SOPA and PIPA to "stifle Internet innovation and protect outdated business models". *Id.* at 23 (*citing* Abigail Phillips, "The 'PROTECT IP' ACT: COICA Redux," The Electronic Frontier Foundation (June 20, 4:31 p.m.) (available at https://www.eff.org/deeplinks/2011/05/protect-ip-act-coica-redux) (wondering whether Viacom would have quashed YouTube had the bill been law at the time)). The second concern, raised primarily by the affected intermediaries themselves, was that the bills would result in a flood of suits by content owners that would overwhelm them and force them to pass on the resulting increased costs to consumers. *Id.* at 23, 127 (citing Letter from American Express et al. to Sen. Patrick Leahy, Chairman, Senate Judiciary Comm. (May 25, 2011) (previously available at http://www.publicknowledge.org/letter-opposing-PIPA-privaterightofaction) (stating that "We believe that the currently proposed private litigation-based process will, however, unintentionally, become a one-side litigation machine with rights owners mass-producing virtually identical cases against foreign domain names for the purpose of obtaining orders to serve on U.S. payment and advertising companies"). As Yeh's paper reports, proponents of the private rights of action responded to the first concern by pointing out that neither PIPA nor SOPA would have allowed private plaintiffs to block domain names or websites like YouTube's, and responded to the second concern by arguing that the tools provided to private plaintiffs under the bills were really quite limited. *Id.* at 24 n. 131 (citing H.R. 3261, the "Stop Online Piracy Act": Hearing Before the H.Comm. on the Judiciary, 112th Cong. (2011) (written statement of Maria Pallante, Register of Copyrights)).

9. *See* Jack C. Schecter, "Online Piracy Legislation—A Cure Worse than the Disease?," Sunstein Kann Murphy & Timbers LLP Intellectual Property Update (Jan. 2012) (available at http://sunsteinlaw.com/online-piracy-legislation-a-cure-worse-than-the-disease/); Mike Masnick, "How SOPA 2.0 Sneaks In A Really Dangerous Private Ability To Kill Any Website," TechDirt (Dec. 16, 2011) (available at http://www.techdirt.com/articles/20111216/03275317104/how-sopa-20-sneaks-really-dangerous-private-ability-to-kill-any-website.html); Patrick McKay, "SOPA, Private Copyright Enforcement Systems, & Free Speech," Fair Use Tube (Jan. 19, 2012) (available at http://fairusetube.org/articles/23-private-copyright) (arguing that the private right of action provisions are the most dangerous provisions in SOPA and PIPA because of the immunity they provide to intermediaries for voluntary actions).

10. *See supra,* Chapter 2: Civil Remedies.

11. *Id.*

12. The relevant provisions of PIPA and SOPA were §4(e) and §103(d)(4), respectively.

13. *See supra,* Chapter 2: Civil Remedies.

14. In the case of SOPA/PIPA, rightsholders who prevailed against an accused foreign rogue site were only permitted to serve the resulting cease and desist orders against payment processors and advertising network

intermediaries; only the Department of Justice was permitted to serve such cease and desist orders on ISPs and search engines.

15. Although some opponents of SOPA and PIPA expressed concern that the absence of a fee- or cost-shifting provision in the bills would lead to large numbers of ruinously expensive actions against foreign websites and intermediaries associated with them, the experience of EU courts in Article 8(3) cases does not provide support for this concern. Although EU courts have so far refused to impose fee- or cost-shifting on a plaintiff in such an action, the number of such actions and the apparent costs associated with them have both been fairly modest to date. *See, e.g.,* Twentieth Century Fox Film Corporation et al. v. British Telecommunications PLC [2011] EWHC 2714 (Ch), [2012] 1 All E.R. 806, Case No. HC 10C04385 (26 Oct 2011) (available at http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/Ch/2011/2714.html&query=Newzbin&method=boolean) (rejecting ISP's demand that plaintiffs pay the costs associated with the ISP's compliance with the court's site-blocking order).

Chapter 4

GOVERNMENT REMEDIES

I. SECTION POSITION

The IPL Section favors legislation authorizing the U.S. Government to conduct investigations and institute criminal and civil enforcement proceedings against Predatory Foreign Websites. The Section also supports legislation granting the U.S. Government the authority to seek issuance of court orders enjoining intermediaries from conducting transactions with Predatory Foreign Websites.

II. SECTION RESOLUTION: TF-08

RESOLVED, the IPL Section supports providing for legislation enabling the U.S. Government to prosecute criminally and/or undertake civil enforcement of copyright piracy and trademark counterfeiting initiated by Predatory Foreign Websites as defined by resolution TF-06 and directed to U.S. end-users/customers.

NOW THEREFORE, the IPL Section supports the enactment of legislation authorizing the U.S. Government to undertake both criminal and civil investigations and enforcement activities against Predatory Foreign Websites, and to seek the issuance of court orders enjoining intermediaries from conducting business with such websites.

III. DISCUSSION

A. Background

One of the challenges posed by extra-territorial Internet piracy is maximizing resources available to enforce intellectual property rights against non-U.S.-based infringing websites. In today's global and increasingly ideas-based economy, the enforcement of intellectual property rights is no longer simply the cost of doing business, but a national economic concern costing the United States billions of dollars each year.[1] Moreover, the proliferation of Internet shopping combined with the high profit margins and perceived low risk from selling infringing goods, has resulted in more prevalent, more sophisticated, and more dangerous counterfeit and pirated goods.[2] Efforts to combat infringement therefore demand a national solution that brings to bear both public and private resources.

The IPL Section examines the federal government's current role in efforts to combat online counterfeiting and piracy, as well as recent legislative proposals that have sought to expand the government's ability to police infringements emanating from beyond U.S. jurisdictional bounds. It explores how balancing a public right of action with a private right of action would best maximize resources available in the combat against extra-territorial online piracy and counterfeiting. This section focuses solely on efforts concerning websites that are based outside of the United States and dedicated to activities that infringe U.S. intellectual property rights.

There is no uniform term to describe foreign websites that engage in online piracy and counterfeiting. For the sake of brevity, this paper will use the term "Predatory Foreign Websites" defined in

the Civil Remedies chapter of this White Paper, which is broad enough to encompass the term of art in each bill discussed below.

B. Government Agencies and Their Role

1. U.S. Customs and Border Patrol ("CBP")

CBP is an agency in the Department of Homeland Security ("DHS"). It is primarily responsible for securing U.S. borders and facilitating lawful international trade and travel, as well as enforcing immigration and drug laws. Its responsibilities include preventing the importation of counterfeit and pirated goods, and enforcing exclusion orders issued by the International Trade Commission ("ITC") pursuant to Section 337 of the Tariff Act of 1930 (19 U.S.C. §1337), which provides relief to U.S. industries from unfair trade practices in importing.[3]

a) Involvement in Online Counterfeiting and Piracy

CBP is generally not involved in policing piracy and counterfeiting on the Internet.[4] CBP may play a role in seizing counterfeit and pirated goods purchased online from Predatory Foreign Websites, but the agency's actions against counterfeiting and piracy in the online world are typically undertaken only in collaboration with other government agencies. For example, as will be explained in more detail below, CBP collaborates with other federal government agencies through the National Intellectual Property Rights Coordination Center (IPR Center).

b) Agency Limitations

Historically, distribution of counterfeit and pirated goods was confined to low-level operators lacking organization and infrastructure, such as street-corner vendors.[5] This primitive distribution model limited the market penetration of counterfeit goods.[6] Today, however, the Internet permits pirates and counterfeiters to reach consumers around the world, 24 hours a day.[7] Counterfeiters, including organized crime syndicates drawn to substantial profit margins from selling pirated and counterfeit goods, are creating websites that appear legitimate in order to deceive consumers into purchasing their illicit wares.

As a consequence of this new e-commerce paradigm, CBP and ICE have reported a great increase in mail and express courier shipments of infringing and counterfeit goods.[8] CBP Commissioner David V. Aguilar has stated that, "The growth of websites selling counterfeit goods directly to consumers is one reason why CBP and ICE have seen a significant increase in the number of seizures at mail and express courier facilities."[9] But the shift from lower volume, heavy shipments of counterfeit and pirated goods, to higher volume, smaller shipments, has strained the CBP's ability to effectively identify and seize illicit goods. The current Director of ICE, John Morton, has suggested that ICE and CBP, "will need to increase surge operations at foreign mail and courier facilities," in order to more effectively police infringement in a world dominated by e-commerce.[10]

2. U.S. Immigration and Customs Enforcement ("ICE")

ICE, like CBP, is an agency of the Department of Homeland Security. ICE was created by the Homeland Security Act of 2002 to serve as the principal investigative arm of DHS.[11] Today ICE is the second largest investigative agency in the federal government. Among other responsibilities, ICE plays an important role in policing the production, smuggling and distribution of counterfeit and pirated products, as well as money laundering associated with criminal IP infringement.[12] ICE's stated goal is to step beyond post hoc enforcement, toward disruption of manufacturing, distribution and financing segments of the criminal organizations that supply infringing goods and content.[13]

Government Remedies

a) Involvement in Online Counterfeiting and Piracy

ICE plays a critical role in government enforcement of intellectual property rights on the Internet. Following the passage of the PRO-IP Act of 2008,[14] which expanded the scope of civil forfeiture remedies for trademark and copyright infringement, ICE has launched a number of operations directed at Internet sites selling or distributing infringing goods and content.

b) Agency Limitations

ICE has taken the position that any domain name registered through a US-based registry is subject to US jurisdiction for copyright or trademark infringement, but ICE's efforts to protect intellectual property on the Internet are limited by the jurisdictional bounds of U.S. law. [15]

3. The National Intellectual Property Rights Coordination Center ("IPR Center")

The ICE-initiated IPR Center has become the vanguard in the government's fight against criminal piracy and counterfeiting. [16] The IPR Center is an inter-agency task force, that was begun by ICE in order to leverage the resources and expertise across the many government agencies that participate in enforcing IP laws. [17] Its stated mission is to address the theft of innovation and manufacturing that threatens U.S. economic and national security, U.S. Industry competitiveness in world markets, and public health.[18] Acting as a "clearinghouse" for investigations into counterfeiting and piracy, the IPR Center draws upon its 19 member agencies, including ICE and CBP, to share information, develop initiatives, coordinate enforcement actions, and conduct investigations of intellectual property theft.[19]

a) Involvement in Online Counterfeiting and Piracy

In June 2010 the IPR Center, spearheaded by ICE, launched the first stage of "Operation in Our Sites."[20] The operation, still ongoing, targets websites selling counterfeit goods and pirated merchandise, as well as those distributing digital copyrighted materials.[21] Subsequent stages of Operation in Our Sites have been timed to coincide with dates on which pirate and counterfeit sales were especially likely to occur (e.g. Cyber Monday, Super Bowl, and Valentine's Day).[22] As of this writing, at least 2,061 domain names have been seized. [23]

Investigators consider several factors to determine which domain names to target, including:

- the popularity of the website, which often correlates with its profitability;
- whether the website is commercial in nature and earns a substantial amount of money—by running advertisements, selling subscriptions, or selling merchandise; and
- whether seizing a site will have a substantial impact on piracy.[24]

Once a suspicious website has been targeted, ICE investigators will obtain counterfeit goods or pirated content from the site, verify with rightsholders that the goods are unauthorized, and apply for a federal seizure warrant based on probable cause. Such a warrant can only be issued by a federal judge, who agrees with ICE that the facts support issuance of a warrant.

As with all judicially authorized seizure warrants, owners of domains seized during Operation in Our Sites have the opportunity to challenge a judge's determination through a petition. Nevertheless, the operation has drawn substantial criticism from free speech and civil liberties advocates. Senator Ron Wyden (D-OR), Representative Zoe Lofgren (D-CA) and groups such as the Electronic Frontier Foundation have denounced the seizures for constitutional violations of free speech and due process.

These complaints, while based on isolated incidents, are not without merit.[25] In case of hip hop blog Dajaz1, the website was shut down on an ex parte basis and censored for over a year before the domain was returned due to a lack of probable cause.[26] Similarly, the website rojadirecta.com was seized despite a lack of significant infringing activity, and was not returned for more than 1.5 years.[27]

The circumstances surrounding Dajaz1 and rojadirecta.com have achieved a level of notoriety among Internet freedom and civil liberties advocates that far surpasses their significance. Such incidents are few in number relative to the amount of seizures overall. [28] Nevertheless, they do suggest caution is necessary where suppression of legitimate speech is a potential consequence of new legislation. [29]

The rise in foreign predatory websites targeting U.S. consumers has heightened the need for the IPR Center to collaborate with international agencies and thereby maximize resources available to combat online counterfeiting and piracy. The IPR Center Outreach and Training Unit conducts domestic training of federal, state, local law enforcement,[30] and works closely with its partner agencies' international attaché networks, local U.S. embassies, INTERPOL, and the World Customs Organization to deliver training and support internationally.[31] The IPR Center also supports the U.S. Patent and Trademark Office's international training events at their Global IP Academy.[32]

b) Agency Limitations

The Internet is a global medium, with millions of websites targeting U.S. Internet users and consumers from foreign territories. Many sites dedicated to selling counterfeits and distributing pirated content to U.S. citizens are registered through registries and registrars outside of the United States and beyond the reach of the IPR Center and its member agencies. Even where a website subject to U.S. jurisdiction is seized, that site may reestablish itself using a foreign domain, thereby undermining the utility of the seizure.[33]

The IPR Center, as a task force, is only as strong as its member agencies. Currently, most of the participating agencies are domestic. While it participates in many international efforts, it will grow in international presence and strengthen international resources as more international organizations join the membership.

4. ITC

The U.S. International Trade Commission ("ITC") is an independent, quasi-judicial federal agency established by Congress with a wide range of trade-related mandates. [34] The ITC adjudicates allegations of unfair acts in connection with imports under Section 337 of the Tariff Act of 1930 as amended, 19 U.S.C. §1337.[35] If the ITC determines that the imports violate Section 337, it may issue an exclusion order barring counterfeit or pirated products from entry into the United States, as well as a cease and desist order directing the violating parties to cease certain actions.[36] CBP enforces the exclusion orders.[37]

Section 337 investigations require formal evidentiary hearings before an Administrative Law Judge (ALJ). The parties conduct discovery, present evidence, and make legal arguments before an ALJ and, ultimately, the ITC. The ITC may review and affirm, reverse, modify, or set aside the ALJ's initial determination, or remand for further proceedings. If the ITC does not review the judge's decision, it becomes the ITC's final determination.[38]

The mission of the ITC is to: (1) administer U.S. trade remedy laws within its mandate in a fair and objective manner; (2) provide the President, the United States Trade Representative (USTR), and Congress with independent, quality analysis, information, and support on matters relating to tariffs and international trade and competitiveness; and (3) maintain the Harmonized Tariff Schedule of the

United States.[39] Intellectual Property-based import investigations represent one of five ways in which the ITC fulfills its mission, but they almost solely deal with physical goods.[40] The primary remedy available in Section 337 investigations is an exclusion order barring the importation of articles connected to particular unfair trade practices such as patent or trademark infringement.[41] In addition, the Commission may issue cease and desist orders against named importers and other persons.[42]

a) Involvement in Online Counterfeiting and Piracy

The ITC has little if any involvement or expertise in policing online infringement. Congress established the ITC as an independent arbiter of whether imported articles violate U.S. intellectual property rights and therefore barred from import into the U.S.[43]

Having said that, the ITC does conduct general fact-finding investigations relating to tariffs or trade at the request of the U.S. Trade Representative, the House Committee on Ways and Means, and the Senate Committee on Finance,[44] and these fact-finding investigations may implicate online counterfeiting and piracy. In fact digital trade is the focus of two 2012-2014 ITC investigations.[45]

b) Agency Limitations

The ITC has concluded that its jurisdiction under Section 337 includes the authority to exclude imports of electronic data transmissions, but this determination does not extend to Internet activity. [46] As explained in more detail below, the Online Protection and Enforcement of Digital Trade Act ("OPEN Act") sought to expand the ITC's jurisdiction to encompass predatory foreign website activity.

C. Attorney General's Right of Action under COICA, PIPA, SOPA, and OPEN

Four major bills relating to Internet piracy and counterfeiting were introduced in Congress in the past two years, yet none have been enacted into law. The four bills include: the Combating Online Piracy and Counterfeiting Act (COICA), the Preventing Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act or PIPA), the Stop Online Piracy Act (SOPA) and the Online Protection and Enforcement of Digital Trade Act (OPEN). Each proposal included a government right of action as a substantial, if not primary, mechanism to combat infringement on the Internet.

1. COCA

COICA[47] was introduced on September 20, 2010 by Senator Patrick Leahy (D-VT), and was the first of a series of major legislative proposals designed to combat online piracy and counterfeiting. The stated purpose of the bill was to "provide the Department of Justice, DOJ, an expedited process for cracking down on websites that traffic in pirated goods or services."[48] To that end, COICA would have authorized the Attorney General to bring an *in rem* action directly against any domain name that resolves to a website dedicated to infringing activities—that is, a website "designed primarily to offer goods or services in violation of federal copyright law, or [for] selling or promoting counterfeit goods or services."[49] The bill required notice to and service on such websites, but did not include any cause of action for private rightsholders.[50]

COICA would have authorized federal law enforcement officers to serve court orders obtained under the Act on three delineated intermediaries;[51]

a. Internet service providers (*e.g.*, VeriSign)[52];
b. Online payment processors (*e.g.*, Visa, PayPal); and
c. Online advertisement providers (*e.g.*, Google's AdWords).

The Act would not have established a program of secondary liability against such intermediaries, rendering them susceptible to criminal or civil charges. Rather, these intermediaries would have only been enjoined to undertake certain remedial actions toward, or discontinue conducting business with a Predatory Foreign Website.

Specifically, online payment processors and advertisement providers could have been required to stop providing of their services to a Predatory Foreign Website, thereby depriving the site of revenue. This indirect enforcement method was seen as a means of overcoming the jurisdictional barriers that prevent legal action against some of the world's most egregious online infringers.

Internet service providers, meanwhile, would have been required to take technically feasible and reasonable steps to prevent a domain name used by a Predatory Foreign Website from resolving to that domain name's IP address. This would have blocked user access to the website in the United States, but not in foreign territories. While this requirement was perceived by some as draconian, it was likely motivated by the fact that many Predatory Foreign Websites, particularly those engaged in distribution of copyrighted digital content, do rely on access to the large number of US users.

A key COICA provision—eventually removed by an amendment—called for the Attorney General to maintain a public list of websites that the Department of Justice determines "upon information and reasonable belief" to be dedicated to infringing activities, but for which no action has been filed.[53] Intermediaries would have received immunity in taking action against websites placed on the list.

2. PIPA

PIPA[54] was introduced by Sen. Leahy in May 2011 as a proposed improvement upon the COICA bill, which failed to pass during the 111th Congress. In contrast to COICA, which authorized the Attorney General to seek injunctive relief only *in rem* against domain names used by Predatory Foreign Websites, PIPA would have also authorized the Attorney General to seek injunctive relief *in personam* against the owners and operators of Predatory Foreign Websites.[55]

PIPA also expanded upon the types of intermediaries subject to court orders under COICA. In addition to Internet service providers (or "Operators… of nonauthoritative domain system servers" in the parlance of PIPA[56]), financial transaction providers and Internet advertising services, PIPA would have permitted court orders to be served on information location tools (i.e. search engines, such as Google or Bing). [57] If served with a court order, a search engine would have been required to de-index a Predatory Foreign Website from its search results.[58]

Unlike its predecessor, PIPA provided copyright and trademark rightsholders with a private cause of action. In one sense, the private cause of action was more expansive than the government cause of action, as it was available against both Predatory Foreign Websites and domestic websites dedicated to infringing activity.[59] But in another important respect, the private cause of action was much more limited. Although both private rightsholders and the Attorney General would have been authorized to serve court orders on financial transaction providers and Internet advertising services, only the Attorney General was authorized to serve court orders on Operators and Information Location Tools.[60]

This dichotomy was apparently designed in recognition that the Attorney General is better incented to consider and protect the many interests that could be affected by court orders to operators and information location tools.[61] Because service providers and search engines could have been asked to block access to information, raising the specter of censorship, it was perhaps appropriate to reserve orders against these intermediaries to the discretion of the Attorney General, who must exercise prosecutorial discretion in doing so.

3. SOPA

SOPA,[62] the House version of PIPA, included substantial modifications[63] but closely tracked the language and substance of PIPA regarding government authority. The Attorney General retained the authority to seek injunctive relief against a Predatory Foreign Website, as well as the authority to serve court orders upon Internet service providers, payment processors, advertising services and information location tools.[64] As with PIPA, private claimants would have only been authorized to enjoin payment processors and advertising services. Although SOPA used different terminology to refer to three of the four intermediaries, the change in terminology was not significant.[65]

4. OPEN

OPEN[66] was introduced as a more palatable alternative to PIPA and SOPA. OPEN would have vested the U.S. International Trade Commission (ITC), rather than U.S. District Courts, with the authority to oversee investigations and disputes against Predatory Foreign Websites. According to Senator Ron Wyden (D-Or), one of the drafters of the Act, "Putting the regulatory power in the hands of the International Trade Commission—versus a diversity of magistrate judges not versed in Internet and trade policy—[would] ensure a transparent process in which import policy is fairly and consistently applied and all interests are taken into account."[67]

OPEN sought to improve upon PIPA and SOPA by narrowing its scope and opening up the bill to commentary by the public. The subject matter was limited to concern predatory foreign websites and did not include domestic websites as PIPA and SOPA had.[68] Although OPEN tracked some of the same language of previous bills, such as allowing orders to be issued on intermediaries similar to those in SOPA and PIPA, it avoided some of their more controversial provisions, such as DNS blocking. Further, while PIPA and SOPA did not include sanctions for abuse of process and discovery, the OPEN Act stated that the Commission could provide such sanctions.[69] However, unlike PIPA and SOPA, only a private complainant would have been authorized to seek orders against intermediaries, and only financial transaction providers and internet advertising services would have been subject to service.[70] Determinations by the ITC were further limited by the authority of the President to nullify them.[71] In addition, the OPEN Act called for cross-departmental cooperation during an investigation by requiring the Commission to consult with and seek information and advice from the Attorney General, the Secretary of State and other officers of trade and intellectual property law enforcement.[72] Such collaboration was intended to maximize governmental resources against online piracy and counterfeiting, and help quell concerns that the ITC may not be properly versed in online piracy and counterfeiting.

D. Public Reaction

Reception to COICA, PIPA and SOPA followed a similar pattern: initially receiving support from copyright and trademark industry leaders and coalitions; appearing on the fast-track to becoming law; then dogged by criticisms from civil libertarians and Internet industry interests; and ultimately abandoned. Often times, critics showed support for the bills' intentions, but opposed their passage because of what many perceived as threats to free speech and due process.

After receiving unanimous approval from the Senate Judiciary Committee in November 2010, COICA was stalled by Senator Ron Wyden (D-OR) in the Senate. Wyden objected to COICA because he believed that it would, "reduce the Internet's ability to promote democracy, commerce and free speech."[73] Other opponents of the bill, including the Center for Democracy and Technology (CDT), the Electronic Frontier Foundation (EFF), and a group of law professors from across the United States, echoed similar sentiments in open letters to Congress, all keyed in on the same policy: DNS blocking.[74]

Evoking by far the most intense criticisms was the provision authorizing the Attorney General to maintain a public list of websites that the Department of Justice determines "upon information and reasonable belief" to be dedicated to infringing activities. Critics derided this provision as a "Blacklist."

The uproar over DNS blocking derived primarily from two concerns. On the one hand, free speech advocates were concerned that DNS blocking would inevitably result in the censorship of non-infringing content. In addition, human rights groups expressed geopolitical concerns, telling Congress that PIPA would lend cover to censorship regimes like China and Iran by betraying America's fight for Internet freedom and expression worldwide. From Reddit to the New York Times, the blocking provisions were likened to the "Great Firewall of China," a euphemism for China's domestic Internet firewall designed to censor websites, and suppress perceived subversive Internet content in that country.

On the other hand, several engineers who were key designers of the early Internet aired concerns that DNS blocking would have destabilizing consequences to the web's underlying architecture. In May 2011 this group published a white paper that was highly critical of the DNS blocking provisions in PIPA, arguing that filters imposed by the bill would be easily evaded, while the presence of a single Predatory Foreign Website on a shared server could disrupt Internet service for every sub-domain, blocking access to infringing and non-infringing sites alike. Moreover, the paper stated that "site redirection envisioned in the [act] is inconsistent with domain name system security extensions," resulting in potential security risks, and destabilizing consequences. Proponents of the bill did weigh in to rebut such criticisms, however.[75]

By the time the OPEN Act was introduced, opposition and support was entrenched along the familiar lines drawn and redrawn with each legislative permutation. Those opposed to the bill, such as the Motion Picture Association of America (MPAA), did not believe that the OPEN Act went far enough to protect U.S. intellectual property rights. In a formal response the MPAA derided the shift in forum to the ITC and the lack of technical means to block access Predatory Foreign Websites from U.S. Internet users. It also said that the legislation would lead to a costly and unnecessary expansion of government bureaucracy.[76]

For the very same reasons opponents criticized the OPEN Act, supporters embraced what they perceived as a balance of the interests between the legitimate concerns of intellectual property rightsholders and Internet openness and freedom. The Library Copyright Alliance applauded the OPEN Act for co-opting a "follow-the-money approach" without compromising the security of the Internet or changing domestic laws.[77] Even major Internet companies, AOL, eBay, Facebook, Google, LinkedIn, Mozilla and Twitter lent their support to the Act by issuing a joint letter to Representative Issa and Senator Wyden.[78]

While the shift to the ITC was a well-intentioned attempt to address censorship concerns, it was likely the OPEN Act's undoing. The ITC was criticized by the RIAA, the Copyright Alliance, and others for moving slowly, even on important cases such as the Apple-Research in Motion case that took 33 months, and *RIM v. Kodak,* which had been filed in January of 2010 and was not ruled on until 31 months later, in July of 2012.[79]

Even tacit supporters of the Act, such as Professor Eric Goldman of Santa Clara University Law School, believed that the administrative agency was an "odd" choice to conduct investigations against Predatory Foreign Websites.[80] The ITC has limited expertise, if any, regarding online counterfeiting and piracy, whereas federal courts have been dealing with such matters for decades. Moreover, as an administrative agency, and not a federal court, there are substantial procedural differences that could lead to important substantive differences.[81] For example, the ITC is not

limited by U.S. District Courts personal jurisdiction, and is not bound by the Federal Rules of Evidence.

Professor Goldman also noted that the ITC has been "gamed" in the patent world, and similar behavior could easily emerge in the realm of copyrights and trademarks.[82] For example, a rights owner chasing a rogue website could simultaneously pursue a domestic court action, a foreign court action and an ITC proceeding.[83] It is unclear how these parallel proceedings would play out in practice when U.S. courts and practitioners are still trying to resolve parallel proceeding problems in patent matters.[84]

IV. CONCLUSION

Although it is beyond the scope of this White Paper to assess the First Amendment and Due Process implications of COICA PIPA, and SOPA, the IPL Section believes that the law on these issues as they pertain to the bills is, at best, ambiguous. Nevertheless the IPL Section acknowledges that the filtering and DNS blocking provisions in those bills are clouded by legitimate concerns. Accordingly, the IPL Section does not adopt any particular recommendation with respect to similar provisions in new legislation.

The IPL Section nevertheless recommends that future legislation against online counterfeiting and piracy include a public right of action that complements a private right of action. Federal government agencies and federal courts have decades of experience in investigating and adjudicating cases involving both online and real-world counterfeiting and piracy operations. Federal agencies possess investigative and collaborative resources that private actors and administrative agencies do not. The IPL Section concludes that the problem posed by Predatory Foreign Websites is one that can only be addressed if the knowledge, experience, and investigative assets of the federal government are brought to bear.

In light of the need for government involvement in combating counterfeiting and piracy, a public right of action should authorize the Attorney General to take investigative action against Predatory Foreign Websites, and allow the Department of Justice to prosecute criminally and/or undertake civil enforcement against Predatory Foreign Websites. Congress should of course ensure that the relevant enforcement agencies have sufficient funding to carry out this important task.

A government right of action must be properly balanced against First Amendment free speech concerns to ensure that non-infringing speech is neither limited nor blocked. Moreover, any remedies must carefully balance due process with intellectual property rights. The IPL Section is confident that the contemplated legislation—allowing the federal government to pursue Predatory Foreign websites and enjoin carefully delineated intermediaries servicing such sites—is consistent with the preservation of an open and innovative Internet.

Notes

1. The Organization for Economic Co-Operation and Development estimates that the United States loses as much as $250 billion to counterfeiting and piracy each year. *See* "Magnitude of Counterfeiting and Piracy of Tangible Products: An Update." OECD, at 1 (Nov. 2009) (available at http://www.oecd.org/industry/ind/44088872.pdf). Intellectual property industries accounting for tens of millions of domestic jobs and as much as 35% of annual U.S. GDP. Economics and Statistics Administration and USPTO, "Intellectual Property and the U.S. Economy," Report, at vii (Mar. 2012) (available at http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf). Copyright and trademark intensive industries alone are estimated to support over 27 million jobs. *Id.* at vi-vii.

2. "Shutting Down Phantom Counterfeiters," *Law360* (Mar. 31, 2009) (available at http://www.law360.com/newyork/articles/94815/shutting-down-phantom-counterfeiters); National Intellectual Property Rights Coordination Center, "Intellectual Property Rights Violations: A Report on Threats to United

States Interests at Home and Abroad" at 4 (2011) (available at http://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/view).

3. CBP's search authority stems from laws such as 19 U.S.C. §§482, 1467, 1496, 1581, 1582.

4. U.S Gov't Accoutability Office, GAO-07-735, "Intellectual Property: Better Data Analysis and Integration Could Help U.S. Customs and Border Protection Improve Border Enforcement Efforts," at 2 n. 4 (2007) (available at http://www.gao.gov/new.items/d07735.pdf) ("Given its role in overseeing the import and export of physical goods, CBP's efforts are primarily directed toward counterfeit goods manufactured overseas and, occasionally, the means to create or finish them in the United States. Computer- or Internet-based piracy of copyrighted media, such as music, movies, or software, is also a significant problem, but because these activities usually have no link to the border, CBP is not as involved in fighting this form of IP infringement.")

5. *See* Nat'l Intellectual Prop. Rights Coordination Ctr, "Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad," at 27 (2011) (available at http://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/view).

6. *Id.*

7. *Id.*

8. CBP Office of International Trade, U.S. Customs & Border Protection Pub. No. 0153-0112, "Intellectual Property Rights: Fiscal Year 2011 Seizure Statistics," at 15 (2012) (available at http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf); Office of International Trade, U.S. Customs & Border Protection Pub. No. 0172-1113, "Intellectual Property Rights: Fiscal Year 2012 Seizure Statistics," at 6 (available at http://www.cbp.gov/linkhandler/cgov/newsroom/publications/trade/fy_2012_final_stats.ctt/fy_2012_final_stats.pdf).

9. Press Release, "CBP, ICE Release Report on 2011 Counterfeit Seizures," CBP (Jan. 9, 2012) (available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/2012_nr/jan_2012/01092012.xml).

10. U.S. Immigration and Customs Enforcement, "Statement of John Morton, Director . . . , Regarding a Hearing on 'Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II,' Before the U.S. House of Reps., Committee on the Judiciary," ("Statement of John Morton") at 18 (Apr. 6, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Morton04062011.pdf).

11. "CBP vs. ICE: The Roles of Two Immigration Agencies," Legal Language Series (Aug. 10, 2011) (available at http://www.legallanguage.com/legal-articles/immigration-agencies-cbp-ice/).

12. Statement of John Morton at 3 (available at http://judiciary.house.gov/_files/hearings/pdf/Morton04062011.pdf).

13. *Id.*

14. Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403122 Stat. 4256 (codified as amended in scattered sections of U.S.C.), (available at http://www.gpo.gov/fdsys/pkg/PLAW-110publ403/pdf/PLAW-110publ403.pdf).

15. Peter Walker, "US anti-piracy body targets foreign website owners for extradition ," *The Guardian (UK)* (July 3, 2011) (available at http://www.guardian.co.uk/technology/2011/jul/03/us-anti-piracy-extradition-prosecution).

16. Press Release, "CBP, ICE Release Report on 2011 Counterfeit Seizures," CBP (Jan. 9, 2012) (available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/01092012.xml).

17. IPR Center, "About Us" (available at http://www.iprcenter.gov/about-us).

18. Statement of John Morton at 4 (available at http://judiciary.house.gov/_files/hearings/pdf/Morton04062011.pdf).

19. Office of the IPEC, "2011 U.S. Intellectual Property Enforcement Coordinator Annual Report On Intellectual Property Enforcement" (Mar. 2012) (available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf).

20. Statement of John Morton at 9 (available at http://judiciary.house.gov/_files/hearings/pdf/Morton04062011.pdf).

21. *Id.*

22. *Id.* at 9-10; *see also* 18 U.S.C. §§981, 2323 (2006); Ryan Singel, "Oops! Copyright Cops Return Seized RojaDirecta Domain Names—19 Months Later," *Wired.com* (Aug. 29, 2012) (available at http://www.wired.com/threatlevel/2012/08/domain-names-returned/).

23. See ICE Press Release, "ICE, CBP, USPIS seize more than $13.6 million in fake NFL merchandize during 'Operation Red Zone'" (Jan. 31, 2013) (available at http://www.ice.gov/news/releases/1301/130131neworleans.htm).

24. Website's Profit Factor Into ICE Calculus of Which Domains to Seize, Electronic Comm. & L. Rep. (BNA) (June 8, 2011) (interview between BNA's Tamlin Bason and Erik Barnett, assistant deputy director of ICE).

25. *See* Jennifer Martinez, "US government dismisses piracy case against Rojadirecta site," *Hillicon Valley* (Aug. 29, 2012) (available at http://thehill.com/blogs/hillicon-valley/technology/246529-us-government-dismisses-case-against-rojadirecta) (Sherwin, Siy, VP of Legal Affairs at Public Knowledge complained, "it is far too easy for the government to seize domain names and hold them for an extended period even when it is unable to make a sustainable case of infringement.").

26. Mike Masnik, "Tell The White House To Stop Illegally Seizing & Shutting Down Websites," *TechDirt* (June 11, 2012) (available at http://www.techdirt.com/articles/20120609/00050419257/tell-white-house-to-stop-illegally-seizing-shutting-down-websites.shtml).

27. Ryan Singel, "Oops! Copyright Cops Return Seized RojaDirecta Domain Names—19 Months Later," *Wired.com* (Aug. 29, 2012) (available at http://www.wired.com/threatlevel/2012/08/domain-names-returned/).

28. Two domain names out of 2061 domain names seized equals 0.097%.

29. Such concerns have also been raised with respect to seizure of domain names for non-copyright purposes. The most prominent example involves another joint operation of ICE and DOJ called "Operation Protect Our Children", which targeted Internet sites promoting child pornography. Unfortunately for clients of the free-hosting Web domain mooo.com, they were inadvertently caught in the Web dragnet when 84,000 of mooo.com's subdomains were seized. *See, e.g.*, Matt Liebowitz & Paul Wagenseil, "Oops! Child-Porn Seizure Shuts Down 84,000 Innocent Sites," *NBC News* (Mar. 30, 2011) (available at http://www.nbcnews.com/id/41649634/ns/technology_and_science-security/t/oops-child-porn-seizure-shuts-down-innocent-sites/#.UUc44tE4VY4). What is less often reported is that all of the "innocent" subdomains not involved in child pornography were returned to their operators within just three days (*id.*), suggesting that the inadvertent mistake was unlikely to have resulted in major harm.

30. Immigration and Customs Enforcement, "National IPR Coordination Center: Outreach and Training Fact Sheet" (undated) (available at http://www.ice.gov/doclib/news/library/factsheets/pdf/outreach-training.pdf).

31. *Id.*

32. *Id.*

33. Ian Paul, "Mozilla Refuses to Help Censor the Internet," *PC World* (May 6, 2011) (available at http://www.pcworld.com/article/227308/mozilla_refuses_to_help_censor_the_internet.html).

34. U.S. International Trade Commission, "FY 2011 AT A GLANCE: General Information" (2012) (available at http://www.usitc.gov/press_room/documents/general_transition.pdf).

35. U.S. International Trade Commission, "Facts and Trends Regarding USITC Section 337 Investigations" (2013) (available at http://www.usitc.gov/press_room/documents/featured_news/337facts.pdf).

36. "U.S. Government Agencies," StopFakes.gov (available at http://www.stopfakes.gov/us-gov-agencies/us-international-trade-commission).

37. *Id.*

38. U.S. International Trade Commission, "FY 2011 AT A GLANCE: Operation 2: Intellectual Property Import Investigations" (2012) (available at http://www.usitc.gov/press_room/documents/op2_transition.pdf).

39. U.S. International Trade Commission, "Mission Statement" (available at http://www.usitc.gov/press_room/mission_statement.htm).

40. U.S. International Trade Commission, "FY 2011 AT A GLANCE: General Information" (available at http://www.usitc.gov/press_room/documents/general_transition.pdf).

41. *Id.*

42. "International Trade Commission Investigations," StopFakes.gov (available at http://www.stopfakes.gov/business-tools/international-trade-commission-investigations).

43. Maria Cantwell et al., "Fighting Unauthorized Trade of Digital Goods While Protecting Internet Security, Commerce and Speech" (undated) (available at http://www.wyden.senate.gov/imo/media/doc/Draft-Discussion-Fighting-the-Unauthorized-Trade-of-Digital-Goods.pdf).

44. USITC Study, "Digital Trade Will Be Focus Of Two New USITC Investigations," News Release 13-004 (Jan. 9, 2013) (available at http://www.usitc.gov/press_room/news_release/2013/er0109ll1.htm).

45. *Id.*

46. Certain Hardware Logic Emulation Systems and Components Thereof, Inv. No. 337-TA-383, USITC Pub. 3089, at 29, (March 1998) (available at http://www.usitc.gov/publications/337/pub3089.pdf).

47. Combating Online Infringement and Counterfeits Act ("COICA") (S. 3804—111th Cong.); *see also* Report by Sen. Judiciary Committee, S. Rep. No. 111-373 (released Dec. 17, 2010) (http://www.gpo.gov/fdsys/pkg/CRPT-111srpt373/pdf/CRPT-111srpt373.pdf). The bill did not pass before the 111th Congress concluded, and thus is no longer pending. *See* http://hdl.loc.gov/loc.uscongress/legislation.111s3804.

48. Congressional Record, Hatch, S.7210.

49. COICA §(2)(b).

50. COICA §(2)(g)(2).

51. While the term "Internet intermediary" cannot be found in the text of COICA, an Internet intermediary is generally understood as a service that facilitates transactions or sharing of information between third-parties on the Internet.

52. COICA somewhat clumsily uses the term "Internet Service Provider" broadly as it is understood in section 512(k)(1) of Title 17, when the bill appears to have intended, based on the obligations imposed, to refer to a subset of such ISPs, namely operators of non-authoritative domain name system servers. PIPA and SOPA are more explicit in this regard.

53. COICA §(2)(j).

54. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PROTECT IP Act" or "PIPA") (S. 968–112th Cong.) was introduced on May 12, 2011. Sen. Leahy released a report (S. Rep. 112-39) on July 22, 2011 explaining the basis for the PROTECT IP Act: http://www.gpo.gov/fdsys/pkg/CRPT-112srpt39/pdf/CRPT-112srpt39.pdf. The bill did not pass before the 112th Congress concluded, and thus is no longer pending. *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.968:.

55. PIPA §§3(a)(1) and (2).

56. PIPA defined "operator" as an operator of a nonauthoritative domain name system server. PIPA §3(d)(2)(A). The primary target of the definition was internet access providers or "ISPs" in common parlance, although domain name registrars that operate domain name servers like GoDaddy would also count as "operators". By contrast, domain name registries like VeriSign operate *authoritative* domain name servers.

57. PIPA §3(d)(2).

58. PIPA §3(d)(2)(D).

59. PIPA §§4(a)(1)(A) and (a)(2).

60. PIPA §3(d)(1) and (2).

61. Statement of Maria Pallante, Register of Copyrights, Before the Committee on the Judiciary, U.S. House of Representatives, 112th Congress, 1st Session, "H.R. 3261, the 'Stop Online Piracy Act" (Nov. 16, 2011) (available at http://judiciary.house.gov/_files/hearings/pdf/Pallante%2011162011.pdf).

62. Stop Online Piracy Act (SOPA) (H.R. 3261–112th Cong.) was introduced on October 26, 2011. The bill did not pass before the 112th Congress concluded, and thus is no longer pending. *See* http://hdl.loc.gov/loc.uscongress/legislation.112hr3261.

63. Among the differences, SOPA allowed targeting of subdomains in search remedies, and its site-blocking requirement focused on generally preventing access by US subscribers to the foreign infringing site, whereas PIPA required ISPs specifically to prevent the site's domain name from resolving to the site's IP address. *See* SOPA §102(c)(2), *cf.* PIPA §3(d)(2).

64. SOPA §102(b)(5).

65. Service Provider" replaced "Operator," "Payment Network Provider" replaced "Financial Transaction Provider," and "Internet Search Engines" replaced "Information Location Tools." The SOPA definitions were coextensive with those in PIPA. The term "Internet Advertising Service" was used in both SOPA and PIPA. *See* SOPA §102(c)(2).

66. Online Protection and Enforcement of Digital Trade Act ("OPEN Act") (S. 2029 and H.R. 3782—112th Cong.) was introduced by the Senate on Dec. 17, 2011 and by the House on January 18, 2012. Current status: http://hdl.loc.gov/loc.uscongress/legislation.112s2029 (Senate version) and http://hdl.loc.gov/loc.uscongress/legislation.112hr3782 (House version). Original version published on the Internet for public comment can be found here: http://keepthewebopen.com/open.

67. "Fighting Unauthorized Trade of Digital Goods While Protecting Internet Security, Commerce and Speech" (undated) (available at http://www.wyden.senate.gov/imo/media/doc/Draft-Discussion-Fighting-the-Unauthorized-Trade-of-Digital-Goods.pdf).

68. OPEN Act §337A(a)(8)(C).

69. *Id.* §337A (i).

70. OPEN Act §337A (g) (1) (A) and (B).

71. *Id.* §337A(e)(4) .

72. *Id.* §337A(c)(3).

73. Rep. Ron Wyden, "Statement for the Record, U.S. Senate Committee on the Judiciary Hearing 'Targeting Websites Dedicated To Stealing American Intellectual Property'" (Feb. 16, 2011) (available at http://www.wyden.senate.gov/priorities/fighting-for-digital-rights).

74. Law Professors, Letter in Opposition to COICA (undated) (available at https://www.eff.org/files/filenode/coica_files/Professors'%20Letter%20re%20COICA%20and%20Signatories.pdf); Peter Eckersley, "An Open Letter from Internet Engineers to the Senate Judiciary Committee," Electronic Frontier Foundation (Sept. 28, 2010) (available at https://www.eff.org/deeplinks/2010/09/open-letter); "Statement of the Center for Democracy & Technology Regarding the Hearing: Targeting Websites Dedicated to Stealing American Intellectual Property," Center for Democracy & Technology (Feb. 16, 2011) (available at https://www.cdt.org/files/pdfs/20110216_rogue_sites_statement.pdf).

75. Some of the rebuttal came from Internet engineering experts who thought the concerns were wrongheaded, misleading or overblown. *See, e.g.,* George Ou, "My DNS Filtering Research before House SOPA Panel" (Dec. 16, 2011) (available at http://www.hightechforum.org/my-dns-filtering-research-before-house-sopa-panel/); George Ou, "DNS Filtering is Essential to the Operation of the Internet" (June 24, 2011) (available at http://www.hightechforum.org/dns-filtering-is-essential-to-the-internet/).

76. Statement of Michael O'Leary, Senior Executive Vice President for Global Policy and External Affairs at the MPAA, "Open Act Ineffective in Targeting Growing Threat of Foreign Criminal Websites," Press Release (Jan. 11, 2012) (available at http://www.mpaa.org/resources/428712e0-704e-4f00-b2ab-2e5c59b35a82.pdf).

77. Library Copyright Alliance et al., Letter to Sen. Wyden, Rep. Issa, and Rep. Chaffetz (Dec. 12, 2011) (available at http://www.arl.org/storage/documents/publications/lca_letteropenact_12dec11.pdf).

78. Joint Letter to Rep. Issa and Rep. Chaffetz (undated), signed by AOL, eBay, Facebook, Google, LinkedIn, Mozilla, Twitter, Yahoo!, Zynga (available at http://keepthewebopen.com/assets/pdfs/12-13-11%20Big%20Web%20Companies%20OPEN%20Endorsement%20Letter.pdf).

79. Susan Decker, "Kodak Loses Case Against Apple, RIM on Imaging Patent," *Bloomberg* (July 20, 2012) (available at http://www.bloomberg.com/news/2012-07-20/kodak-loses-case-against-apple-rim-on-imaging-patent.html); *see also* Jamie Keene, "RIAA call online piracy a threat to national security," *The Verge* (Jan. 6, 2012) (available at http://www.theverge.com/2012/1/6/2686593/riaa-rejects-open-confirms-sopa-support); Chloe Albanesius, "Amidst SOPA, PIPA Blackouts, Issa Introduces Rival OPEN Act," *PCMag.com* (Jan. 18, 2012) (available at http://www.pcmag.com/article2/0,2817,2399070,00.asp); Sandra Aistars, "The Alternative is Impractical," *New York Times* (Jan. 18, 2012) (available at http://www.nytimes.com/roomfordebate/2012/01/18/whats-the-best-way-to-protect-against-online-piracy/the-open-act-is-impractical-for-artists).

80. Eric Goldman, "The OPEN Act: Significantly Flawed But More Salvageable Than SOPA/PROTECT-IP" (Dec. 10, 2011) (available at http://blog.ericgoldman.org/archives/2011/12/the_open_act_de.htm).

81. *Id.*

82. *Id.*; *see also* Colleen V. Chien, "Patently Protectionist? An Empirical Analysis of Patent Cases at the International Trade Commission," 50 Wm. & Mary L. Rev. at. 63 (2008) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1150962).

83. Eric Goldman, "The OPEN Act: Significantly Flawed But More Salvageable Than SOPA/PROTECT-IP" (Dec. 10, 2011) (available at http://blog.ericgoldman.org/archives/2011/12/the_open_act_de.htm).

84. *Id.*; *see also* Colleen V. Chien, "Patently Protectionist? An Empirical Analysis of Patent Cases at the International Trade Commission," 50 *Wm. & Mary L. Rev.* at. 63 (2008) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1150962).

Chapter 5

VOLUNTARY ACTION

I. SECTION POSITION

The IPL Section supports the development of voluntary industry programs to combat Internet-based copyright and trademark infringement by Predatory Foreign Websites. The IPL Section also supports the enactment of legislation aimed at deterring intellectual property infringement and encouraging voluntary industry initiatives as a part of a multi-pronged approach to addressing Internet-based infringement.

II. SECTION RESOLUTION: TF-09

RESOLVED, that the IPL Section supports voluntary efforts to combat Internet-based copyright and trademark infringement by Predatory Foreign Websites, as defined by Resolution TF-06, including through mechanisms such as streamlining and expediting submission and processing of nonjudicial infringement complaints, implementation of online nonjudicial complaint forms and automatic takedown tools, and development of programs designed to educate Internet users about intellectual property rights and to deter infringing activity;

FURTHER RESOLVED, that the IPL Section supports the development of robust and proactive voluntary industry programs to identify and remove infringing content, and to deny access to counterfeited products and/or disassociate with infringing activity, such as voluntary content filtering by hosting sites and partner website vetting by ad networks and payment processors; and

FURTHER RESOLVED, that the IPL Section supports the enactment of legislation aimed at deterring Internet-based intellectual property infringement and encouraging voluntary industry initiatives and wider adoption of such initiatives, both in the United States and around the world, as part of a multi-pronged approach to reduce the harm caused by illegal activities of Predatory Foreign Websites.

III. DISCUSSION

A. Background: Voluntary Industry Initiatives to Combat Online Piracy and Counterfeiting ("Voluntary Action")

In the United States, following the collapse of efforts to pass the Protect IP Act ("PIPA")[1] and the Stop Online Piracy Act ("SOPA")[2] proposals in 2012, public discussion has expanded to include whether voluntary industry initiatives to combat online piracy and counterfeiting undertaken by Predatory Foreign Websites ("PFWs")[3] could represent an effective and feasible resolution to the continuing problem. The PIPA and SOPA bills were aimed at preventing counterfeits offered by and pirated works made available on foreign websites from reaching U.S. consumers by obligating or strongly encouraging intermediaries, such as Internet service providers ("ISPs"), Internet advertisers, payment processors and search engines, to take action by limiting access or financial support to such sites. Opposition to the bills was widely debated, ultimately caused both bills to be withdrawn, and rallied opponents to challenge vociferously other measures designed to protect copyrights and trademarks on the Internet. This debate has focused the spotlight on intermediaries

and voluntary industry initiatives, as the government and private sector grapple with striking a balance between (1) providing adequate enforcement mechanisms for trademark and copyright owners and (2) maintaining the freedom and openness commonly associated with the Internet in the United States.

As the focus on voluntary industry initiatives has increased over the past two years, several main categories of Internet-focused policy responses have emerged. Such strategies range in scope and effectiveness and many include mechanisms such as the implementation of online complaint forms or the creation of hybrid gradual response systems that might result in suspension of an individual's Internet service. While none of these measures represent a definitive solution to the online piracy and counterfeiting issue, they potentially offer tools that could be used as part of a multi-pronged approach together with legislation, to reduce illegal activities being conducted or offered by PFWs through their websites and online services.

Any discussion of voluntary industry initiatives must examine the relevant industries' incentives for adopting those strategies. Essentially, do sufficient incentives exist for intermediaries to embrace, implement, and promote voluntary measures to deter PFWs from continuing their operations? If not, would it help to implement legislation to encourage voluntary measures, for instance to shield such intermediaries from liability for certain reasonable steps taken to address PFWs?

B. Current Copyright and Trademark Legal Framework

1. The Digital Millennium Copyright Act

The Digital Millennium Copyright Act ("DMCA"), enacted in 1998, incentivizes certain categories of intermediaries to share in the burden of copyright enforcement compliance by limiting their liability for the infringing activities of their users. Prior to the enactment of the DMCA, ISPs and website operators were potentially exposed to copyright infringement liability because every time a user accessed infringing content, the provider's server reproduced a copy of protected material.[4] Under the 1976 Copyright Act, any reproduction of a copyrighted work without consent of the copyright holder that is not excused by an exception or limitation to copyright constitutes copyright infringement.[5] ISPs also were exposed to claims of secondary liability for their users' infringing reproductions and distributions.[6] The safe harbor provisions of the DMCA grant ISPs immunity from liability for monetary damages (although not from limited injunctive relief) for material transmitted, edited, or posted by a user.[7] In order to qualify for immunity, an ISP must expeditiously remove identified infringing material in response to a takedown notice submitted by a copyright holder[8] or if/when the ISP has actual or red-flag[9] knowledge of the presence of infringing material or activity on its server.[10] As a condition of eligibility, ISPs must also designate an agent to receive infringement notifications, implement a reasonable repeat infringer policy, and accommodate standard technical measures.[11]

The safe harbor provisions allow websites such as YouTube and Facebook—which primarily rely on user-submitted content—to operate without facing potentially expansive civil liability related to copyright infringement. The safe harbor provisions were explored and explained in a recent dispute between Viacom (as the content owner) and YouTube (as the service provider). Viacom brought suit against YouTube in the Southern District of New York alleging that YouTube induced users to engage in copyright infringement, "directly, vicariously or contributorily[,] subject to damages of at least $1 billion . . ., and injunctions barring such conduct in the future."[12] YouTube, "an online video hosting service that enables users to share their personal and original video clips across the Internet through websites, mobile devices, blogs, and electronic mail,"[13] claimed immunity under the safe harbor provisions of the DMCA; YouTube argued that it was immune as long as

it timely responded to takedown notices from copyright holders.[14] YouTube also argued that the burden of policing copyright infringement rested with the copyright holder, and YouTube had no duty to search for infringing material on its site.[15]

In June 2010, the court granted summary judgment in favor of YouTube and found that it qualified for protection under the DMCA safe harbor provisions as long as it continued to remove infringing material upon notification.[16]

Viacom appealed to the Second Circuit,[17] which vacated the district court's summary judgment decision, concluding that a jury could have found that YouTube had actual knowledge of the infringing content, although additional fact finding on this issue was required.[18] The Second Circuit also concluded that the "District Court erred by interpreting the 'right and ability to control' provision to require 'item specific' knowledge."[19] It also found that three of the four software functions that YouTube performs fall within the DMCA safe harbor, but that further fact finding was required on the fourth function.[20]

In reaching this decision, the Second Circuit explained the distinction between "actual knowledge" and "red flag knowledge," [21] noting that Viacom's arguments conflated the two, and held that "actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor."[22] The court also held that the common law doctrine of "willful blindness" may be applied "in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under §512(c)(1)(A)," but remanded the case to the District Court for further fact-finding on this point.[23] Finally, the court also suggested that the safe harbor might not apply if a service provider were found to have had the "right and ability to control access" to the infringing activity, which requires "something more than the ability to remove or block access to materials posted on a service provider's website."[24] The case was remanded to the district court for further fact-finding on this point and on the question of whether YouTube had received a financial benefit directly attributable to the infringing activity.[25] Therefore, while the Second Circuit's decision more specifically defined instances in which the DMCA's safe harbor provision would not apply, it also affirmed that general awareness of infringing activity was not sufficient to trigger liability for website operators. On remand, the district court considered additional factual submissions provided by the parties about: 1) whether YouTube had "knowledge or awareness of any specific infringements;" 2) whether YouTube "willfully blinded itself to specific infringements;" 3) whether YouTube had the "right and ability to control infringing activity" as required by the DMCA; and 4) whether any of the clips-in-suit were syndicated to a third party.[26]

The court rejected Viacom's proffered argument that YouTube's claims to the statutory safe harbor under the DMCA as an affirmative defense shifted the burden of proof to YouTube to prove each element of its defense, including that it lacked knowledge of the allegedly infringing content. Instead, the court explained that the DMCA's purpose was to require copyright owners to provide specific notice to service providers, thus enabling the removal by the service provider of the allegedly infringing content.[27] The DMCA specifically assigns the burden of discovery and enforcement on the copyright owner.[28]

Similarly, the court found that YouTube had not been willfully blind by failing to see the myriad examples of infringing activity occurring on its site.[29] In order to be willfully blind, there must have been specific examples of infringement that had been identified, about which the service provider failed to act.[30] The court clarified further:

To find [allegedly infringing content using specific search terms, as Viacom suggested] would require YouTube to locate and review over 450 clips [in this case]. The DMCA excuses YouTube

from doing that search. Under §512(m), nothing in the applicable section of the DMCA shall be construed to require YouTube's "affirmatively seeking facts indicating infringing activity."[31]

Finally, the court explained that the "mere knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that, the provider must influence or participate in the infringement."[32]

Accordingly, while recent decisions have discussed the applicability of certain exceptions to the DMCA's safe harbor provisions to specific fact patterns, the divergence of opinions among various courts considering digital copyright enforcement cases suggests that the "correct" application of the DMCA is far from obvious. While intermediaries can generally avoid liability by providing mechanisms through which copyright owners can report alleged instances of copyright infringement, and by subsequently taking steps to remove such content where appropriate,[33] many copyright pirates have found ways to utilize the safe harbor provisions as loopholes and online infringement continues largely unfettered. Although the current legal structure creates a powerful incentive for intermediaries to cooperate voluntarily, the primary enforcement burden still falls on the copyright owner, who must constantly patrol the Internet for infringements. Unfortunately, rightsholders often find that, without further cooperative measures from ISPs such as takedown-staydown policies or content filtering, the same copyrighted titles continue to be infringed on the same sites over and over again.

Moreover, recent proposals made by Maria Pallante, the Register of Copyrights, during a speech at Columbia University[34] and later during a hearing before the House Judiciary Committee. Subcommittee on Courts, Intellectual Property and the Internet,[35] suggest that a major overhaul of the Copyright Act may be warranted in light of the dramatically evolved Internet environment through which many works now travel. Indeed, Rep. Goodlatte (R-VA) has taken up the challenge and announced on April 24, 2013, that the House Judiciary Committee has launched a comprehensive review of copyright law to determine whether it adequately protects copyrights in "the digital age,"[36] particularly in light of online distribution, breakdowns in licensing payments due to rampant unauthorized online distribution, orphan works, statutory licensing and damages.[37] As a result, the DMCA's current structure and/or mandates may evolve over the next several years as lawmakers attempt to bring the entire Copyright Act up to date with respect to digital works.

2. DMCA Requirements vs. Recent Voluntary Initiatives in the Copyright Field

While the DMCA provides incentives for ISPs and other such parties to voluntarily implement notice and removal procedures for online copyright infringement, it does not by itself represent a voluntary industry initiative. Instead, it is a statutory mandate which ISPs must follow if they wish to take advantage of the safe harbors from liability for monetary damages provided under the Act. However, the methods by which some intermediaries have implemented this mandate are helpful in understanding the choices intermediaries have made (or can make) of purely voluntary actions to reduce counterfeiting and piracy undertaken on their systems. Questions remain regarding the scope and effectiveness of truly voluntary industry initiatives that have been implemented to date. To the extent that certain strategies have proven to be effective, they can potentially serve as key components of a more comprehensive and uniform legislative plan for combating the continued reach of PFWs into the U.S. market.

An example of an independent voluntary initiative that has been successfully implemented is YouTube's Content ID program.[38] This program allows copyright owners to easily identify and manage their content on YouTube and provides them with streamlined mechanisms for preventing or otherwise expediently removing copyright infringing content online.[39] Videos uploaded to YouTube are scanned against a database of files that have been submitted by content owners.[40]

Voluntary Action

Content owners may choose to monetize, block or track the identified video.[41] When Content ID identifies a match between a video and a file in this database, it applies the policy chosen by the content owner.[42] In addition, copyright owners can use separate online copyright infringement complaint forms provided by YouTube in the event they identify a particular infringing video(s) that they wish to have removed from the site.[43]

Despite robust programs voluntarily developed by the likes of YouTube, eBay, and others, such initiatives have not been uniformly adopted and implemented throughout the United States, let alone the rest of the world. As a result, copyright owners are forced to navigate a patchwork system of DMCA-oriented takedown procedures and independently-created voluntary initiatives in order to attempt to police and enforce the appropriate use of their copyrighted works. Absent implementation of new legislation that creates greater uniformity among such initiatives, the burden that falls on copyright owners will only continue to grow, as new technologies rapidly evolve beyond the scope of protections and safe harbors currently covered by the DMCA, and which may make policing efforts less centralized and more expensive.

3. No DMCA-type Legislation in the Trademark Field

Unlike copyright law, no U.S. trademark law currently exists that codifies a notice and takedown procedure for combating trademark abuse. While the DMCA requires ISPs desiring to take advantage of the safe harbor to provide mechanisms for reporting alleged *copyright* infringement and to remove such content after receiving notice, it does not extend to alleged *trademark* infringement. As a result, ISPs and other online industry leaders have been slow to create, implement and make available mechanisms for reporting trademark infringement occurring online. While service providers have had streamlined online complaint systems for reporting copyright infringement in place for years because of the DMCA, they have only recently started to follow suit with regard to the provision of similar forms and procedures for reporting trademark infringement, even without a statutory mandate.[44]

This shift in policy has been driven, in part, by recent court decisions that have placed online trademark infringement issues in the limelight.

In one such case from 2010, *Tiffany, Inc. v. eBay, Inc.*,[45] the Second Circuit affirmed that trademark owners carry the burden of policing and reporting counterfeit items and infringing content when their products are sold or advertised in an online marketplace.[46] In that case, Tiffany sued eBay for trademark infringement, trademark dilution, and false advertising.[47] Tiffany asserted that a high volume of counterfeit jewelry was being sold under the famous "TIFFANY" name in eBay's online marketplace, and that eBay's responses to its complaints about such counterfeiting activities were insufficient.[48] Tiffany contended that eBay was liable for operating a marketplace that it knew was used to sell substantial quantities of goods that infringed a trademark, even if it did not know which particular goods were being infringed.[49]

In rejecting Tiffany's argument, the Second Circuit affirmed that a generalized knowledge of impropriety was insufficient to establish liability.[50] Instead, under established precedent, online marketplaces like eBay were only required to remove listings that they specifically knew were auctioning counterfeit or infringing merchandise.[51] In reaching this decision, the Second Circuit emphasized that eBay and other online marketplace companies have a strong financial incentive to minimize the counterfeit goods sold on their websites.[52]

Under the principles outlined by the Second Circuit, the burden currently falls on the trademark owner to monitor and report infringing content with specificity in order for liability to attach to an

intermediary for failure to act on a report of infringement. This mirrors the operation of the DMCA. Although notice compliance is not codified in trademark law as it is in copyright law (with the DMCA), except in the context of the Anti-Cybersquatting Consumer Protection Act ("ACPA"),[53] common law has begun to provide similar parameters regarding what obligations website operators must undertake toward trademark claims, which helps to explain why many website operators have been motivated recently to implement voluntary initiatives targeting trademark infringement.[54]

C. Current and Proposed Voluntary Industry Initiatives

The Internet's structure and breadth raises numerous challenges for traditional IP enforcement against PFWs, including the current legal framework, jurisdictional hurdles, anonymity of operators, high enforcement costs, and the ease with which infringing operations can be relocated and resumed.[55] Due to these challenges, rightsholders are exploring and experimenting with new strategies to bolster enforcement mechanisms and curb online infringement and counterfeiting, especially potentially involving in this process intermediaries that support the operation of PFWs.[56] Some of these strategies have already shown promise as valuable tools in a multi-pronged approach to curtailing the activities of PFWs. The implementation of these voluntary initiatives also highlights areas for improvement and enhanced cooperation, the importance of shared responsibility across rightsholders and relevant industries in addressing PFWs, and the continued need for legislation to incentivize cooperation, all of which are essential in truly impacting the predatory business practices of PFWs.[57]

1. Current Initiatives

Although it is too soon to definitively conclude which approaches are most effective, many voluntary enforcement strategies have shown promise, and should continue to serve as valuable tools in a multi-pronged approach that includes voluntary industry initiatives. These include:

a) Online Infringement Complaint Forms and Processes

Over the last few years, many ISPs and App marketplace providers have created and implemented online complaint forms that provide both copyright and trademark owners with a streamlined procedure for reporting and affecting the takedown of infringing content online.[58] The availability of this process, however, does not shift the burden of policing marks and copyrighted content from the intellectual property owners to the ISPs or other online marketplace providers.[59] Instead, copyright and trademark owners must still independently monitor and report infringing/counterfeit activity and conduct follow-up as necessary, regardless of how many times infringing content or counterfeit listings are reposted in different forms, thus increasing the potential cost of enforcement as online marketplaces continue to multiply.

These online forms and procedures are not uniform across ISPs and online marketplace providers, and vary in terms of efficiency and effectiveness. Some parties, like Google,[60] will conduct a limited investigation into reasonable trademark infringement complaints and, in appropriate circumstances, terminate repeat infringers. Other providers, like Apple, have embraced a less aggressive approach and have instead sought to forward complaints to a developer to provide the parties with an opportunity to reach an agreement before taking any independent action to remove content at issue.[61]

In order for copyright or trademark owners to increase the likelihood of having content or listings at issue removed, they must review the particular ISP or marketplace provider's posted procedures and requirements in detail and follow any instructions stringently. Failure to do so can often result in a delayed response or no response to a takedown request. It is also important to note that the

various ISPs and marketplace providers are almost constantly updating and refining these forms, and thus their procedures can differ from visit to visit, and their average response times can vary.

b) Restrictions on Internet Access and Hybrid Approaches

In addition to online forms and procedures for removing infringing content, many proposed industry initiatives have focused on ways to block Internet access to such content and/or suspend Internet privileges altogether for their subscribers who repeatedly engage in infringing activity online based on terms and conditions governing user participation in that site.[62] A broad spectrum of such restrictions, ranging from traffic shaping to blocking to outright suspension of Internet access, have been proposed and even implemented in some cases.[63] Most of these strategies only target copyright infringement at this time, and do not expressly address trademark infringement issues. Noteworthy restriction strategies can be summarized as follows:

(1) Suspension

Suspension is a severe remedy imposed by an ISP directly. If an ISP identifies an Internet subscriber who engages conduct that violates its terms and conditions, including for instance, engaging in infringing activity, that ISP may alert the subscriber of his/her unauthorized conduct and suspend that subscriber's Internet connection to access the Internet for a set period of time.[64] Some ISPs, such as Qwest, have been employing the suspension strategy for repeat copyright infringers for several years.[65] Such ISPs have generally only suspended Internet service in instances where a repeat infringer has been identified, notified of its noncompliance and yet continues to abuse the service.[66]

(2) Traffic Shaping

Traffic shaping, also sometimes referred to as "throttling,"[67] occurs when an ISP reduces the bandwidth provided to an Internet user.[68] If an ISP receives notice or otherwise becomes aware of infringing activity, it can engage in traffic blocking to effectively reduce the speed or the volume of traffic of the user at issue.[69] This strategy has been employed to varying degrees by a wide array of parties over the last decade, including by many universities seeking to reduce the amount of illegal file-sharing by students.[70]

(3) Content Identification, Blocking and Filtering

Blocking and filtering are processes used by ISPs to restrict Internet users from accessing websites that contain infringing content.[71] ISPs accomplish this by using protocols (*e.g.* P2P), ports, and various software programs to identify infringing content and prevent users from accessing, posting and/or otherwise sharing such content.[72]

A number of user-generated content ("UGC") sites in particular employ content identification and filtering to *proactively* prevent infringements from occurring and/or recurring on their platforms. YouTube, Dailymotion, and Youku for instance utilize their own proprietary or licensed content recognition technology to filter videos posted by users upon upload and to block copyrighted content that is not authorized by the copyright owner from being published to those sites.[73] YouTube's content filter is used by more than 4,000 media companies and has identified more than 200 million copyrighted videos.[74] It seems a number of major UGC sites recognize that by sharing in the burden of monitoring for infringements they help "to foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners," to "strike a balance that, on a going-forward basis, will result in a more robust, content-rich online experience for all," thus serving UGC sites' own business interests.[75] These same content recognition technologies also power the authorized monetization of copyrighted content on UGC sites.

While ISP blocking activities have been fairly limited in the United States to date, blocking and filtering has been widely attempted and, in some cases, court ordered in various European countries.[76] In both the United States and Europe, many critics of the blocking/filtering approach contend that serial infringers understand the technology being employed and can easily evade these measures.[77] Further, many critics contend that filtering/blocking measures often end up preventing access to legal, non-infringing content.[78] It bears noting that blocking measures were debated in the U.S. Congress prior to the January 2012 Internet Blackouts that nominally protested the inclusion of DNS blocking mechanisms.[79]

(4) Hybrid Approaches (Educational Initiatives)

Given the widespread nature of online piracy and the inherent weakness of individual approaches to combating such unlawful conduct, the focus in both the United States and other international jurisdictions has turned to the creation and implementation of hybrid enforcement programs. These programs typically consist of a number of steps, whereby an Internet user is first provided with a series of alerts if they access or share infringing content. The intent is to educate Internet users about what constitutes copyright infringement and how it negatively impacts others and the economy.

The main example in the United States is the recently-launched U.S. Copyright Alert System[80] (also called a "Stepped Enforcement Approach"). This program was launched in early March 2013 to help consumers understand illegal distribution through peer-to-peer ("P2P") networks and educate them about unlawful content sources. It is the result of voluntary cross-industry cooperation between the 5 major U.S. Internet access providers (*e.g.* Comcast, Verizon) and the music/film/TV content creator industry (*e.g.* RIAA, MPAA, IFTA, A2IM).[81] It represents a mutual recognition that such cooperation is necessary "to prevent, detect, and deter Online Infringement."[82] The Copyright Alert System sets up a framework for an enhanced education, notice, and enforcement program which entails a multi-step process[83] of progressive alerts to ISP subscribers whose IP addresses are discovered to be engaged in infringing activities on P2P networks and mitigation measures for repeat infringers, with a clear focus on educating users and changing consumer behavior.

It also gives ISP providers a range of mitigation measures (*e.g.* temporary reduction in Internet speed, temporary restriction of Internet access, etc.) and a high degree of flexibility and autonomy in selecting mitigation measures.[84]

2. Voluntary Best Practices in the U.S.

While Internet intermediaries[85] are not required by law to take the initiative to uncover instances of infringement or counterfeiting, or to decrease the use of their services by infringers, several have developed sets of "best practices" to decrease the prevalence of this conduct using their services.

a) Payment Processors

Because of low barriers to entry, ease of operations, decreased risk of identification and criminal prosecution, and limited effectiveness of civil IP enforcement, the Internet provides PFWs a target-rich environment for profiteering from illegal sales and distribution of copyrighted and trademarked goods.[86] PFWs that sell counterfeit products or offer subscriptions to access infringing content (on a streaming or downloading basis) rely on legitimate payment processors to conduct their illegal sales transactions. These credible payment processors lend an air of legitimacy to PFWs and may dupe unsuspecting consumers into purchasing counterfeit goods or paying for access to pirated content while costing the U.S. billions in lost revenue.[87]

Voluntary Action

Partnerships, such as the one between the International Anti-Counterfeiting Coalition ("IACC") and the major card networks (MasterCard, Visa International, Visa Europe, PayPal, American Express and Discover/Pulse/Diners Club), allow concerned rightsholders to streamline reports of counterfeit sellers utilizing these payment options.[88]

If a payment processor determines that a website has engaged in widespread infringement, the payment processors can suspend or terminate payment services to that website's merchant account.[89] This initiative has demonstrated success, with 906 individual merchant accounts terminated during one year of IACC member referrals.[90]

Individual payment processors, such as American Express, Visa, MasterCard and PayPal also have systems in place to report illegal conduct undertaken by authorized merchants.[91]

Payment Processors, of course, face financial and reputational risk, including damage to their own brand and loss of consumer trust, when associated with PFWs. These risks incentivize Payment Processors to participate in voluntary initiatives to prevent the use of their services on PFWs. Nevertheless, there are challenges to effective enforcement through this initiative, including preventing terminated merchants from re-registering with a card network through a different acquiring bank and the use of sophisticated technologies by counterfeit sellers to prevent investigative transactions.[92] Thus, while a cooperative partnership is in place between the prominent card networks and rightsholders, the PFWs continue to evolve to evade enforcement. Additional legislative enforcement tools and increased pressure on these PFWs are essential to stemming the flow of revenue to these illicit operations.

b) Online Advertisers and Advertising Networks

In addition to the sale of counterfeit products and paid memberships to access copyrighted content, PFWs also rely on advertisements to monetize their infringing operations. In the recent indictment against the operators of the MegaUpload group of sites, prosecutors alleged that online advertising on MegaUpload and its associated websites, which relied heavily on copyrighted content to lure visitors to the site, earned an estimated $25 million.[93] Recent university studies have also detailed how online ad networks support PFWs and how the ads of unsuspecting prominent advertisers appear on these PFWs.[94]

The online advertising ecosystem is complex and consists of many parties involved in the serving of a given ad to any website, legitimate or infringing.[95] This presents challenges of transparency, whereby advertisers may be unaware, in fact, of precisely where their ads appear online. The advertising industry has responded to the challenge of providing transparency into the advertising value chain by implementing Quality Assurance Guidelines for Networks & Exchanges (QAG).[96] This initiative aims to clarify the marketplace for advertisers, increase buyer control of ad placement and promote brand safety. Ad networks and exchanges that voluntarily self-certify to adhere to the guidelines commit to provide advertisers with clear ad placement details. In the current iteration of the QAG, the category of illegal content prohibited from sale by compliant networks and exchanges, includes content that infringes copyrights. The guidelines do not apply to other parties involved in the advertising value chain (*e.g.*, ad servers that are indirectly involved in the serving of an ad to a publisher website).[97]

Another initiative aimed at addressing the issue of advertising on PFWs is the ongoing work on behalf of the Office of the Intellectual Property Enforcement Coordinator ("IPEC"). IPEC is encouraging private industry to establish best practices in order to prevent advertisements from appearing on PFWs and to remove such websites from their inventory.[98] IPEC is also involved in industry negotiations for a broader approach to curb advertising associated with infringing content or counterfeit goods.[99]

Within its support pages, Google posts its policy for reporting copyright infringement for websites utilizing its Google AdSense service.[100] Google expressly reserves the right to terminate an AdSense publisher's participation in the program if it receives a notice or otherwise has reason to believe that the publisher's website is infringing.[101] While Google's AdSense policy demonstrates progress, many in the content community have complained that Google does not do enough to cut off advertising services for websites that facilitate piracy or counterfeiting.[102] What also remains unclear is whether and how Google plans to expand its AdSense policy across all of the products and services it owns in the display ad ecosystem.[103]

Expanding best practices beyond networks and exchanges to cover all relevant players in the advertising ecosystem, establish measures to prevent advertisements from appearing on PFWs in the first place, and provide a streamlined referral processes to report advertisement-supported infringements, will enable players in the online advertising ecosystem and rightsholders to share in the responsibility of preventing ad revenue from flowing to PFWs. Legislation may be necessary to drive that result.

c) Advertisers and Ad Agencies

The American Association of Advertisers ("4As") and the Association of National Advertisers ("ANA") recognize the threat to brand integrity and consumer trust by the placement of ads on PFWs.[104] In a joint initiative, the 4As and ANA have strongly encouraged their members to take affirmative steps to prevent U.S. advertisers from appearing on such websites.[105] These affirmative steps include, for example, language in ad placement contracts that requires ad networks and other intermediaries involved in U.S.-originated advertising campaigns to take commercially reasonable measures to prevent ads from appearing on PFWs.[106] Other steps include requiring intermediaries involved in the serving of an advertisement to expeditiously respond to complaints by rightsholders or advertisers and provide remediation to advertisers for advertisements misplaced on PFWs.[107]

These affirmative steps, if combined with industry-wide best practices[108] that address the *entire* online advertising ecosystem and supporting legislation, would provide enhanced tools to prevent advertising revenue from flowing out of the U.S. market to PFWs.

d) Mobile App Marketplaces

Currently, the development, distribution, and sale of software applications for smartphones, tablets, and mobile devices ("Apps") is a burgeoning field. The major marketplaces for such apps are maintained by major companies, including Apple (iTunes),[109] Google (Play), Amazon (App Store), and Microsoft (Windows Phone store). These marketplaces allow third-party software developers to submit apps for distribution and sale to users for either a small fee or free. The various app stores generally cite intellectual property issues in their criteria for eligibility for developers to (1) maintain their status as developers for the platform; and (2) to submit and distribute apps through the company's store platform.

Many App marketplace providers have created and implemented streamlined online complaint forms for copyright and trademark owners to use to request removal of infringing content and apps. These forms and procedures are ever-evolving, and have improved significantly in terms of both effectiveness and average response time over the last two years. It is important to note, however, that the forms and procedures differ between providers. Rightsholders must recognize and strictly adhere to the technical requirements for submitting a complaint set forth by each marketplace provider in order to improve the chances of receiving a prompt and satisfactory response.

Voluntary Action

(1) Google Play

Following the online submission of an infringement complaint regarding Google Play Apps, Google conducts its own investigation, removes the App if it believes that the content at issue is infringing, and then notifies the developer of the removal.[110] If the complainant does not own any existing copyright or trademark registration and/or the content at issue is only somewhat similar to the complainant's cited work or mark, it is much more likely that Google will not remove the content, but will instead notify the complainant that it believes the facts support removal and directs the complainant to conduct any desired follow-up with the App developer directly.[111]

(2) Apple's App Store

Until recently, IP owners had to contact Apple through a dedicated email address (appstorenotices@apple.com) in order to submit complaints and takedown requests regarding alleged copyright and trademark infringement occurring in the App Store. However, beginning in late 2012, Apple launched a new online infringement complaint form that largely mirrors already existing forms provided by other marketplace providers.[112]

Apple forwards these complaints to the allegedly infringing party first and provide complainant's contact information in an effort to have the parties work out a resolution independently. [113] If no resolution is reached or if the infringing party does not respond, only then will Apple conduct its own examination and potentially remove the content at issue.[114]

(3) Facebook's App Center

Facebook launched its App Center in 2012.[115] Shortly, after launching this new App marketplace, Facebook implemented an online complaint form that allows users to submit claims for both trademark[116] and copyright infringement.[117] The online form is not limited to Facebook's App Center, and can also be used for reporting allegedly infringing content found anywhere on Facebook (*e.g.,* Facebook profile pages—which are often used by companies to promote particular products/services, etc.).

(4) Amazon's App Center for Android

Amazon launched its App Center for Android on March 22, 2011.[118] According to Amazon's Appstore director, "Customers have used the Amazon Appstore to test drive and buy millions of apps and games for their Kindle Fire and other Android devices in the first year alone."[119] Amazon also reported a dramatic increase in App sales after its Kindle Fire was launched into the market.[120] Amazon's Appstore offers the option to report potential copyright infringement but does not appear to have a notice and take down provision for reporting trademark infringement or counterfeiting.[121]

Amazon has a policy expressly prohibiting the sale of stolen goods, recopied media (including movies and music), promotional media, recopied or transferred video games, recopied software and "replicas" of trademarked items through Amazon's sites.[122] Amazon reserves the right to "summarily remove or alter it without returning any fees the listing has incurred" and "make judgments about whether or not content is appropriate."[123]

(5) Safe Harbor Issue with App Takedowns

One notable downside with these processes is that marketplace providers do not have any safe harbors from claims that they unlawfully interfered with App developers' rights (such as free speech if a parody were the type of work removed), even where the marketplace provider believes it had a good faith basis for agreeing with the complainant's position. In this area, legislative clarification would be helpful.

e) Search Engines

Search engines play an important role in driving Internet user traffic to both legitimate and illicit goods and content. In an effort to prevent consumer confusion as to the legitimacy of copyrighted content on the Internet and promote legitimate content-providing services, such as Netflix and Hulu, rightsholders are actively submitting search removal requests to Google, Bing and other search engines. These notices identify specific search results that link to infringing material and request removal of these links from search engine results.

Similarly, sites selling counterfeit versions of products bearing the rightsholders' trademarks are often delivered as high-ranking search results, or results promoted because of keyword advertising. In such cases, Google has argued that using trademarks to serve advertising in sponsored links does not qualify as a "use in commerce" and thus does not constitute infringement.[124] The Second District court in *Rescuecom* disagreed with Google's position and found that Google's display, offering and selling of plaintiff's mark to Google's advertising customers qualified as a "use in commerce." [125] Following the ruling of the court, the parties in this matter settled the case.[126] Nevertheless, rightsholders may submit complaints to Google for links in the sponsored ad results that violate a brand's trademark. Google will then investigate these complaints and may restrict the use of the trademark in Google's ad campaigns.[127]

Google publishes copyright removal referrals it receives from copyright owners and reporting organizations in its Google Transparency Report.[128] According to this report, between March 1 and March 14, 2013, Google received over 15 million requests to de-list search links to content on approximately 3,700 domains.[129] These referral requests were sent on behalf of over 2,500 copyright owners.

In a press release issued in August 2012, Google announced it would begin to factor in the number of copyright removal requests a website received in its search algorithm.[130] According to Google, this would cause websites which receive a high volume of removal notices to appear lower in Google's search result rankings and "should help users find legitimate, quality sources of content more easily."[131]

In testing that claim, the RIAA measured over six months the impact of its Google search removal requests and the ranking of the referred websites in search. The findings published by the RIAA were not encouraging and ultimately found "no evidence that Google's policy has had a demonstrable impact on demoting sites with large amounts of piracy."[132] Rights owners invest substantial time and resources in sending such a high volume of search removal requests pertaining to PFWs but it seems to have little impact on the prevalence of PFWs in search returns.[133] According to Google's Transparency Report, the site for which Google has received the most removal requests (over 4.3 million in the past year) is filestube.com,[134] which apparently continues to receive over 17% of its upstream traffic directly from Google Search results.[135]

f) Domain Registrars and Domain Proxy Services

Historically, domain-name based anti-infringement initiatives, like the Uniform Domain-Name Dispute-Resolution Policy ("UDRP"), have focused on addressing trademark infringements contained in domain names themselves, offering relief only in the case of PFWs who infringe brands in their choice of domain names (e.g. www.piratedDisneymovies.com). However, several U.S.-based domain registrars, such as GoDaddy, have created and implemented streamlined complaint forms for the submission of broader complaints of trademark or copyright infringement.[136] Penalties for violating the terms of services of such registrars, including through copyright and trademark infringement, may involve a suspension of the registrar services that will lead to a disruption in the PFWs operations.

Other registrars, such as eNom, do not offer online forms, but instead provide instructions for users to submit copyright infringement claims via email or standard mail.[137]

Similarly, many proxy domain name registrars have also recently created and have begun to offer online complaint forms for consumers (*e.g.* GoDaddy's Domains by Proxy's inclusion of a "File a Claim" tab on its homepage).[138] Proxy registrars such as Namecheap's WhoisGuard or Domains by Proxy allow users to register a domain name without having to reveal their personal contact information to the public. This service serves many legitimate uses, such as preventing spam to publicly listed contact details, but it is also used to mask identifying information for operators engaging in criminal activity.[139]

U.S.-based proxy registrars, such as WhoisGuard and Domains by Proxy, may terminate their proxy service for operators of PFWs who violate the proxy services terms and conditions of use, including if a PFW is engaged in copyright and trademark infringement.[140] If revoked, the privacy shield on the registrant's details is removed and these details are published in the public WHOIS database.[141] While voluntary cooperation by U.S.-based domain registrars and domain proxy services is encouraging, a large number of PFWs use rogue registrars and proxy services, such as Fundacion Private Whois in Panama,[142] which do not accept referrals of copyright and trademark infringement and, thus, do not share operator details or terminate service for such violations.

There are ongoing efforts to develop enhanced recordkeeping and vetting of domain name registrants. These efforts, involving numerous parties such as the Internet Corporation for Assigned Names and Numbers ("ICANN"), aim to require domain name registrants to provide accurate contact information at the time of registration and would provide for termination by the registrars of registrants who fail to respond to inquiries about the accuracy of such information, as well as possible disclosure of registrant details in response to a legitimate infringement complaint. [143]

ICANN, industry leaders and government organizations are also working on best practices for newly-released generic top-level domains ("gTLDs").[144] In particular, these parties are developing guidelines that will require enhanced diligence of WHOIS records and data and certification of the validity of such information.[145] The new guidelines will also require registrars to immediately remove infringing content or otherwise disable a domain if a website engages in infringing activity.[146] Even if these guidelines are successfully implemented, they do not address already existing gTLDs and issues with registrars will remain.

g) Online Marketplaces

Online marketplaces and auction sites like eBay have also implemented online complaint procedures for copyright and trademark owners to report infringing or counterfeit activity.

Under eBay's Verified Rights Owner ("VeRO") Program,[147] for example, an IP owner can download and submit a Notice of Claimed Infringement (NOCI) to eBay's designated agent if it has a good faith belief that its work has been copied in a way that constitutes copyright or trademark infringement.[148] Highlights of the program include:

- Expeditious removal of listings reported to eBay by more than 5,000 intellectual property rights owners;
- Proactive monitoring and removal of listings that violate eBay policies designed to prevent the listing of infringing items on eBay;
- Suspension of repeat offenders; and
- Cooperation with rights owners seeking personal information on alleged infringers.[149]

Although the VeRO has been widely used by intellectual property owners since its inception in the mid-2000s, the program has not been without its critics. In particular, many public complaints have been voiced about eBay's alleged lack of a legitimate internal investigation and widespread misuse of VeRO program by parties seeking to remove content that does not actually violate their IP rights.[150]

IV. CONCLUSION

The overarching challenge is to develop and implement a multi-pronged solution which is effective, efficient, and replicable across jurisdictions. In order to be both effective and politically feasible, the approach must be proportionate, fair, provide due process, respect fundamental rights and avoid unreasonably impacting third parties.

In order to accomplish this objective, rightsholders, service providers and Internet intermediaries must focus on raising awareness of what constitutes infringing content, educate the public about available reporting mechanisms for identifying infringing content, offer affordable legal alternatives, and enhance incentives for intermediaries to take affirmative steps to address PFWs.[151]

To date, a number of voluntary industry initiatives to combat infringing and counterfeiting activities are already underway. Some of these initiatives have successfully enhanced the ability of copyright and trademark owners to enforce expediently and effectively their intellectual property rights. Most notably, YouTube's ContentID program and associated takedown tools, and eBay's VeRO program have provided copyright and trademark owners with effective mechanisms for efficiently dealing with infringing content and counterfeit goods.

Educational initiatives, such as the Copyright Alert System and industry-driven voluntary best practices among payment processors and advertising entities appear to offer a significant degree of promise that a politically feasible and financially reasonable solution may be achieved.

However, these moderately effective mechanisms are not sufficient on their own to combat PFWs. For example, while companies like Apple and Google conduct their own independent investigations upon receipt of a copyright or trademark infringement complaint, the factors these investigation teams actually evaluate when considering infringement claims and making content removal determinations have not been publicly disclosed.

Tools designed merely to streamline submission of infringement notifications do not go far enough. Even with such enhanced tools, under the legal framework of the DMCA and existing trademark precedent, rightsholders bear the entire burden of patrolling for infringements by PFWs. A broader approach that involves intermediaries sharing in the burden of addressing PFWs benefits the U.S. economy as a whole and reduces the prevalence of infringing and counterfeited products that erode the market share of legitimate rightsholders who also offer their content, goods and services to U.S. consumers.

Given that voluntary industry initiatives have produced some successes but have also fallen short in many respects, legislation that enhances the effectiveness of, and incentivizes expansion upon, these initiatives or that creates greater uniformity among such efforts would represent an effective and feasible approach to curtailing online infringement and counterfeiting by PFWs.

Finally, provided that such a solution seeks to balance the competing interests in the online world, it could result in cooperative efforts to stop the outflow from the U.S. to overseas of not only content and goods, but also the money that encourages PFWs to continue their infringing (but highly lucrative) activities.

Notes

1. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PROTECT IP Act" or "PIPA") (S. 968—112th Cong.), introduced on May 12, 2011. Sen. Leahy released a report (S. Rep. 112-39) on July 22, 2011 explaining the basis for the PROTECT IP Act: http://www.gpo.gov/fdsys/pkg/CRPT-112srpt39/pdf/CRPT-112srpt39.pdf. The bill did not pass before the 112th Congress closed, and thus is no longer pending: http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.968:.
2. Stop Online Piracy Act ("SOPA") (H.R. 3261—112th Cong.), introduced on October 26, 2011. The bill did not pass before the 112th Congress closed, and thus is no longer pending: http://hdl.loc.gov/loc.uscongress/legislation.112hr3261.
3. For a complete discussion of this chapter's use of the phrase "Predatory Foreign Websites," *see generally* the Civil Remedies chapter, and specifically, Resolution TF-06.
4. Jonathan Zittrain, *A History of Online Gatekeeping*, 19 *Harv. J. L. & Tech*. 253, 263-265 (2006).
5. 17 U.S.C. §106 (2006).
6. *Id.*
7. 17 U.S.C. §512 (2006).
8. *Id.*
9. The phrase "red flag knowledge" does not appear in the statute itself, but has become the accepted shorthand way of referencing Section 512 (c)(1)(A)(ii), which states that an internet service provider's (ISP's) duty to remove infringing content is triggered when the service provider becomes aware of "facts or circumstances from which infringing activity is apparent." This provision is distinct from Section 512 (c)(1)(A)(i)'s requirement that an ISP remove material upon receiving "actual knowledge that the material or an activity using the material on the system or network is infringing." *See* Senate Judiciary Committee Report, S. Rep. No. 105-190 (1998) at 44-45 ("Subsection (c)(1)(A)(ii) can best be described as a 'red flag test,'"); House Committee on Commerce Report, H.R. Rep. No. 105-551, part 2 (1998) at 53-54. For a discussion of the difference between the two types of knowledge, *see, e.g.*, the blog post by Naomi Jane Gray, "The Second Circuit Finds the Beef," *Shades of Gray Law* (July 13, 2012) (available at http://www.shadesofgraylaw.com/2012/07/13/2nd-circuit-finds-the-beefreverses-summary-judgment-grant-in-youtube/#more-532).
10. *See* 17 U.S.C. §512(a) (2006).
11. *See id.* §512(c)(2) (designated agent), §512(i)(1)(A)—(B) (reasonable repeat infringer policy and standard technical measures).
12. Viacom Int'l, Inc. v. YouTube, Inc., 253 F.R.D. 256, 259 (S.D.N.Y. 2008) (summarizing basis of lawsuit).
13. Viacom Int'l, Inc. v. YouTube, Inc., No. C-08-80211, 2009 WL 102808, at *1 (N.D. Cal. Jan. 14, 2009) (in the context of Viacom's motion to compel third party discovery in California, describing YouTube's services).
14. *Id.* at *2.
15. *See, e.g., id.*
16. Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 529 (S.D.N.Y. 2010).
17. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012).
18. *Id.* at 26 & 34.
19. *Id.*
20. *Id.*
21. *Id.* at 31-32 ("[T]he actual knowledge provision turns on whether the provider actually or 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person.").
22. *Id.* at 32.
23. *Id.* at 41-42.
24. *Id.* at 38.
25. *Id.*
26. Viacom, Int'l v. YouTube, Inc., 940 F. Supp. 2d 110, 112 (S.D.N.Y. 2013).
27. *Id.* at 114-15 ("The Act places the burden of notifying such service providers of infringements upon the copyright owner or his agent."); *id.* at 115 ("Thus, the burden of showing that YouTube knew or was aware of the specific infringements of the works in suit cannot be shifted to YouTube to disprove. Congress has determined that the burden of identifying what must be taken down is to be on the copyright owners, a determination which has proven practicable in practice.").

28. *Id.*
29. *Id.* at 115-17.
30. *Id.* at 116; *see also id.* at 116-17 ("Here, the examples proffered by plaintiffs (to which they claim YouTube was willfully blind) give at most information that infringements were occurring with particular works, and occasional indications of promising areas to locate and remove them. The specific locations of infringements are not supplied: at most, an area of search is identified, and YouTube is left to find the infringing clip.").
31. *Id.* at 117.
32. *Id.* at 118.
33. This includes online access providers, web hosting providers, content hosting or listing platforms (like YouTube and eBay), search engines and indexes, but does not extend to advertising networks and other online advertising entities or to payment providers.
34. Maria A. Pallante, "The Next Great Copyright Act," Twenty-Sixth Horace S. Manges Lecture, Columbia University (Mar. 4, 2013) (available at http://www.law.columbia.edu/null/download?&exclusive=filemgr.download&file_id=612486).
35. Maria A. Pallante, "The Register's Call for Updates to U.S. Copyright Law," Testimony before U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Courts, Intellectual Property & the Internet (Hr'g Mar. 20, 2013) (available at http://www.copyright.gov/regstat/2013/regstat03202013.html).
36. House Judiciary Comm. Press Release, "Chairman Goodlatte Announces Comprehensive Review of Copyright Law" (Apr. 24, 2013) ("The goal of these hearings will be to determine whether the laws are still working in the digital age.") (available athttp://judiciary.house.gov/index.cfm/press-releases?ContentRecord_id=1B5C521A-D006-B517-9949-43E692E1E52E).
37. *Id.*
38. *See* "How Content ID Works" (available at http://support.google.com/youtube/bin/answer.py?hl=en&answer=2797370 or http://www.youtube.com/t/contentid).
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. *See* "YouTube Copyright Complaint" (available at http://youtube.com/yt/copyright/copyright-complaint.html).
44. *See, e.g.*, Katja Weckstrom, "Liability for Trademark Infringement for Internet Service Providers," 16 *Marq. Intell. Prop. L. Rev.* 1, 5 (2012); Michael Leonard & John Sullivan, "Combating Trademark i-Nfringers: Practical Strategies for Enforcing Brands in Apps," *World Trademark Review* at 47 (Oct./Nov. 2011) (available at http://www.worldtrademarkreview.com/Issues/Article.ashx?g=bb11215a-0313-4851-b191-d3836fb9d3a1).
45. 600 F.3d 93 (2d Cir. 2010).
46. *Id.* at 107-108.
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.* at 107 ("For contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary."); *see also* Viacom v. Tiffany line of cases discussed above.
51. Tiffany, Inc. v. eBay, Inc., 600 F.3d at 107. The Second Circuit also corrected Tiffany's argument based on Inwood Labs. v. Ives Labs, Inc., 456 U.S. 844 (1982), clarifying that *Inwood* does not establish contours of the "knows or has reason to know" prong, and only confirms that liability can exist if a defendant "continues to supply its product to *one* whom it knows or has reason to know is engaging in trademark infringement." *Id.* at 108. The Second Circuit also denied Tiffany's argument that specific knowledge (and therefore liability) is established by its demand letters and DMCA take down letters; instead, the Second Circuit found that the demand letters and take down notices did not identify specific sellers of these counterfeit goods and that eBay removed listings from sellers it found to be counterfeiting and suspended repeat offenders from access to the site. *Id.* at 109. Under these circumstances, the court confirmed that Tiffany failed to demonstrate "that eBay was supplying its service to individuals who it knew or had reason to know were selling counterfeit Tiffany goods." *Id.*
52. *Id.* at 109 ("But we are also disposed to think, and the record suggests, that private market forces give eBay and those operating similar businesses a strong incentive to minimize the counterfeit goods sold on their

websites. eBay received many complaints from users claiming to have been duped into buying counterfeit Tiffany products sold on eBay. . . . The risk of alienating these users gives eBay a reason to identify and remove counterfeit listings. Indeed, it has spent millions of dollars in that effort.") (internal citations omitted).

53. 15 U.S.C. §1125(d). Domain name registrars are afforded a safe harbor under the ACPA for "refusing to register a domain name, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name," as long as they were acting in compliance with a court order under 15 U.S.C. §1125(d) or implementing a "reasonable policy of the registrar . . . prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark." 15 U.S.C. §1114(2)(D).

54. If a website operator fails to respond to reports filed by trademark and/or copyright owner concerning specific instances of alleged infringement, it can be found liable for contributory infringement. Such liability has created an incentive for website operators to create reporting mechanisms and procedures that provide trademark and copyright owners with a means of reporting infringing activity and getting such content removed. *See, e.g.,* Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 658 F.3d 936 (9th Cir. 2011) (affirming finding of liability for contributory trademark infringement and copyright infringement by web host Akanoc, which had received eighteen notices of specific infringement claims from Louis Vuitton but neither responded to these notices nor removed the infringing content).

55. Kristina Montanaro, Executive Summary, "IACC Payment Processor Portal Program: First Year Statistical Review," International AntiCounterfeiting Coalition at 2 (Oct. 2012) (available at http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf).

56. *See* Testimony of Christine N. Jones (Executive Vice-President, General Counsel, & Corporate Secretary, The Go Daddy Group, Inc.) before the Senate Judiciary Committee Hr'g on "Targeting Websites Dedicated to Stealing American Intellectual Property" (Feb. 16, 2011) (available at http://www.judiciary.senate.gov/pdf/11-2-16%20Jones%20Testimony.pdf).

57. *See also* P. Bernt Hugenholtz, "Codes of Conduct and Copyright Enforcement in Cyberspace," Copyright Enforcement and the Internet at 303 (2010) (available at http://www.ivir.nl/publications/hugenholtz/Codes_of_conduct.pdf).

58. *See, e.g.,* eBay's VERO program (http://pages.ebay.com/vero/notice.html and http://pages.ebay.com/againstcounterfeits/index.html); Apple iTunes and App Store (http://www.apple.com/legal/intellectual-property/); Amazon's Appstore for Android (http://www.amazon.com/gp/help/customer/display.html/ref=hp_rel_topic?ie=UTF8&nodeId=508088#copyright).

59. *See generally,* Viacom Int'l v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012); Tiffany, Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).

60. *See, e.g.,* "Google Play Trademark Infringement Policy" (available at http://support.google.com/googleplay/android-developer/answer/141511?hl=en).

61. *See* "iTunes Content Dispute" (available at http://www.apple.com/legal/internet-services/itunes/appstorenotices/).

62. The IPL Section takes no position on whether an ISP blocking access to a particular site is within its rights to do so. However, the ISP's own terms and conditions relating to its subscribers' activities—which typically are deemed accepted when a user signs up for services (at which point the terms and conditions are available to the user) and begins using the site—may authorize such blocking if a subscriber engages in conduct prohibited by the terms and conditions. *See e.g.* 2 Ian Ballon, *E-Commerce and Internet Law* §§23.01-23.03 (2012).

63. Internet Society, *Perspectives on Policy Responses to Online Copyright Infringement* (available at http://www.wipo.int/edocs/mdocs/copyright/en/wipo_isoc_ge_11/wipo_isoc_ge_11_ref_00_runnegar.pdf) (last visited March 13, 2013).

64. This measure has been employed as the final step in an escalating "graduated response" process (otherwise known as "three strikes") by various European countries. *See* Annemarie Bridy, "Graduated Response American Style: 'Six Strikes' Measured Against Five Norms," 23 *Fordham Intell. Prop. Media & Ent. L.J.* 1-66 (2012).

65. *See* "Qwest ISP Piracy Suspension" (available at http://news.cnet.com/8301-31001_3-10444879-261.html).

66. *Id.*

67. Bandwidth throttling is a control technique employed by communications networks to regulate traffic by intentionally slowing service, frequently in order to limit network congestion and prevent server crashes and/or to regulate users' bandwidth usage. See, e.g., "Bandwidth Throttling," Wikipedia (available at https://

en.wikipedia.org/wiki/Bandwidth_throttling) (last visited June 10, 2013); Damon Brown, "AT&T Wireless Bandwidth Throttling: The Backlash Has Begun," *PCWorld* (Feb. 14, 2012) (available at http://www.pcworld.com/article/249952/atandt_wireless_bandwidth_throttling_the_backlash_has_begun.html); Chloe Albanesius, "Is Your ISP Throttling Bandwidth? Google Will Know," *PCWorld* (Jan. 28, 2009) (available at http://www.pcmag.com/article2/0,2817,2339772,00.asp).

68. Jeremy F. DeBeer and Christopher D. Clemmer, "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?," 49 *Jurimetrics* 4 (2009).

69. *Id.*

70. *See* Juran Janus, "Congress Looks At Technology's Role In Addressing Illegal File-Sharing On University Campuses," IEEE USA Today's Engineer (July 2007) (available at http://www.todaysengineer.org/2007/Jul/filesharing.asp).

71. *See* Michael S. Sawyer, "Filters, Fair Use, and Feedback: User-Generated Content Principles and the DMCA," 24 *Berkeley Tech. L.J.* 363 (2009) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1369665).

72. Sanna Wolk, "Filtering and Blocking of Copyright Infringement Works: A European Perspective," *Inha Int'l Forum* 33 (2012) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2186751).

73. *See* "YouTube Content ID" (available at http://www.youtube.com/t/contentid); "Dailymotion Content Protection" (available at http://www.dailymotion.com/legal/contentprotection); "YouKu Joins Broad Coalition in Support of UGC Principles," *PR Newswire* (Mar. 7, 2011) (available at http://www.prnewswire.com/news-releases/youku-joins-broad-coalition-in-support-of-ugc-principles-117512623.html).

74. *See, e.g.*, discussion of YouTube's Content ID Program, *above*; Emir Efrati, "Reappearing on YouTube: Illegal Movie Uploads," *The Wall Street Journal* at B1 (Feb. 7, 2013) (available at http://online.wsj.com/article/SB10001424127887324906004578290321884631206.html).

75. Principles for User Generated Content Services (undated) (available at http://www.ugcprinciples.com).

76. Courts in the United Kingdom have recently "ordered ISPs to block access to The Pirate Bay and Newzbin2, both file-sharing sites found by the courts to facilitate infringement on a massive scale." *See* "Cases Wrestle with Role of Online Intermediaries in Fighting Copyright Infringement," Center for Democracy & Technology (June 26, 2012) (available at https://www.cdt.org/policy/cases-wrestle-role-online-intermediaries-fighting-copyright-infringement).

77. *See* Public Knowledge, "Filtering Whitepaper: Limitations and Consequences" (undated) (available at http://www.publicknowledge.org/paper/pk-filtering-whitepaper_3); *see also* Mike Masnick, "As Expected, BitTorrent Providers Planning To Route Around Comcast Barrier," *Tech Dirt* (Feb. 18, 2008) (available at http://www.techdirt.com/articles/20080215/171450267.shtml).

78. *Id.*

79. *Compare* Testimony of David Sohn (Senior Policy Counsel, Center for Democracy & Technology) before the House Committee on the Judiciary, Subcommittee on Intellectual Property, Competition and the Internet, on "Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites (Part 1)," Tr. at 29 (Mar. 14, 2011) (arguing that "there are serious technical and cybersecurity concerns. For example domain name blocking is technically incompatible with DNSSEC, which is a standard for protecting the security of the domain name system that has been a decade in the making and is just rolling out. In addition, the technologies that users—or, excuse me, the techniques that users would employ to circumvent blocking would create new cybersecurity risks as well.") (available at http://judiciary.house.gov/hearings/printers/112th/112-153_65186.PDF) *with* Testimony of Daniel Castro (Senior Analyst, Information Technology and Innovation Foundation), before same, Tr. at 43 (Mar. 14, 2011) ("Some opponents of better enforcement of IP claim this will disrupt the Internet. I am here to tell you this claim is 100 percent false. The simple fact is that using DNS to block access to websites or servers is not particularly new or challenging. DNS redirection has been used for many years to block spam and bot nets and to protect users from malware. It is also widely used to provide parental control filters, correct typos in URLs and to provide improved search results.") (available at http://judiciary.house.gov/hearings/printers/112th/112-153_65186.PDF).
See, also, Electronic Frontier Foundation, "SOPA/PIPA: Internet Blacklist Legislation" (undated) (available at https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill); Center for Democracy & Technology, "The Perils of Using the Domain Name System to Address Unlawful Internet Content" (Sept. 2011) (available at https://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf); Grant Gross, "SOPA Author to Remove ISP Blocking Provision," *PC World* (Jan. 13, 2012) (available at http://www.pcworld.com/article/248171/sopa_author_to_remove_isp_blocking_provision.html).

80. *See* "What is a Copyright Alert?" (2013) (available at http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/).

81. Although RIAA and MPAA are well-known acronyms, IFTA and A2IM are not so well-known; IFTA stands for the Independent Film and Television Alliance, and A2IM stands for the American Association of Independent Music. *See* Daniel Bean, "Entertainment and Internet Providers Launch Copyright Alert System," *ABC News* (Feb. 27, 2013) (available at http://abcnews.go.com/blogs/technology/2013/02/entertainment-and-internet-providers-launch-copyright-alert-system/).

82. *See* Copyright Alert System Memorandum of Understanding (July 6, 2011) (available at http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf).

83. The Copyright Alert System gives the ISP providers a range of acceptable mitigation measures (*e.g.* temporary reduction in Internet speed, temporary restriction of internet access, etc.) and flexibility in selecting mitigation measures, and early reports indicate difference in which mitigation measures will be deployed by the various ISPs. *See* Eriq Gardner, "Internet Providers Launch Copyright Alert System," The Hollywood Reporter (Feb. 25, 2013) (available at http://www.hollywoodreporter.com/thr-esq/internet-providers-launch-copyright-alert-424231). The Copyright Alert System does not require ISPs to terminate subscribers' accounts under any circumstances, but does not prohibit them from doing so.

84. Kevin Roose, "The Internet's 'Six Strikes' Rule Is About to Clamp Down on Your Illegal Downloads," *New York Magazine* (Feb. 7, 2013) (available at http://nymag.com/daily/intelligencer/2013/02/explaining-the-internets-six-strikes-rule.html).

85. The concept of Internet intermediaries is discussed and defined in more detail in the Civil Remedies section of this White Paper.

86. Kristina Montanaro, Executive Summary, "IACC Payment Processor Portal Program: First Year Statistical Review," International AntiCounterfeiting Coalition at 2 (Oct. 2012) (available at http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf).

87. Press Release, "IACC has New Tools to Cut Off Money to Bad Sites," International AntiCounterfeiting Coalition (undated) (available at https://iacc.org/news-media-resources/press-releases/iacc-has-new-tools-to-cut-off-money-to-bad-sites.php).

88. IACC, "Payment Processor Initiative & Portal Program" (undated, initiative launched January 2012) (available at http://c.ymcdn.com/sites/members.iacc.org/resource/resmgr/IACC_PaymentProcessorInitiat.pdf).

89. *See* Future of Music Coalition, "Payment Processor Best Practices for Online Copyright Infringement: What it Means for Musicians" (Oct. 24, 2011) (available at http://futureofmusic.org/article/article/payment-processor-best-practices-online-copyright-infringement).

90. Kristina Montanaro, Executive Summary, "IACC Payment Processor Portal Program: First Year Statistical Review," International AntiCounterfeiting Coalition at 2 (Oct. 2012) (available at http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf).

91. *See* Testimony of Denise Yee (Senior Trademark Counsel, Visa Inc.) before U.S. Senate, Committee on the Judiciary (Hr'g Feb. 16, 2011) (available at http://www.judiciary.senate.gov/pdf/11-2-16%20Yee%20Testimony.pdf); Testimony of Maria A. Pallante (Acting Register of Copyrights, U.S. Copyright Office) before U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Intellectual Property, Competition and the Internet (Hr'g Mar. 14, 2011) (available at http://www.copyright.gov/docs/regstat031411.html); International Trademark Association "Best Practices for Addressing the Sale of Counterfeits on the Internet" (Sept. 2009) (available at http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf) (American Express, MasterCard, Visa, Discover, and PayPal as participating PSPs).

92. Testimony of Denise Yee at 2.

93. U.S.A. v. Kim DotCom, Megaupload Ltd, et al., Crim. No. 1:12CR3, Indictment (E.D. Va. filed under seal on Jan. 5, 2012) (available at http://thenextweb.com/insider/2012/01/20/heres-the-full-72-page-megaupload-doj-indictment/).

94. Jon Taplan, "Advertising Transparency Report," U. So. Cal. Annenberg Innovation Lab (Feb. 13, 2013) (available at http://www.annenberglab.com/viewresearch/45); Dawn C. Chmielewski, "Report Links Google, Yahoo to Pirate Sites," *The Los Angeles Times* (Jan. 2, 2013) (available at http://articles.latimes.com/2013/jan/02/entertainment/la-et-ct-piracy-ads-20130102).

95. Terence Kawaja, Display LumaScape, LUMA Partners LLC (undated) (available at http://www.lumapartners.com/lumascapes/display-ad-tech-lumascape/).

96. IAB, Networks & Exchanges, Quality Assurance Guidelines v. 2.0 (July 2013) (available at http://www.iab.net/media/file/QualityAssuranceGuidelines7252013.pdf).

97. *See* Copyright Alliance, "Best Practices Make Best Partners" (May 3, 2012) (available at http://www.copyrightalliance.org/2012/05/best-practices-make-best-partners).

98. IPEC, 2012 Annual Report on Intellectual Property Enforcement at 33 (Mar. 2012) (available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf); *see also* IPEC, Joint Strategic Plan for Intellectual Property Enforcement (June 20, 2013) (available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf). IPEC endorsed the final v.2.0 version of the QAG, although the MPAA and other rightsholder groups were critical of the changes made from earlier versions. *Compare* http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting (July 15, 2013) *with* http://variety.com/2013/biz/news/mpaa-scoffs-at-new-anti-piracy-plan-1200562813/(July 15, 2013),

99. *See, e.g.,* IPEC, "Advertisers and Advertising Agencies Address Online Infringement Through Best Practices," Spotlight (Mar. 2012) (available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/spotlight/ipec_spotlight_may_jun_spotlight_2012.pdf).

100. *See* "Google AdSense Copyright Infringement Policy" (undated) (available at http://support.google.com/adsense/bin/answer.py?hl=en&answer=9892).

101. *See id.*

102. *See, e.g.,* Sandra Aistars, "Google Shows Its True Colors?" Copyright Alliance (May 18, 2011) (available at http://www.copyrightalliance.org/2011/05/google-shows-its-true-colors/#.Ua5pVthj-ke); Ben Sheffner, "How Google Profits from Illegal Advertising," MPAA Blog (Jan. 12, 2012) (available at http://blog.mpaa.org/BlogOS/post/2012/01/10/How-Google-profits-from-illegal-advertising-and-keeps-the-money-even-after-getting-caugh.aspx); RIAA, "One Year Later: Google's Report Card on Making Copyright Work better Online" (Dec. 19, 2011) (available at http://76.74.24.142/423B769B-66EE-B137-CDED-F44741C19E6B.pdf).

103. *See, e.g.*, Brian Womack and Sara Forden, "Google Said to Face New Antitrust Probe Over Display Ads," Business Week (May 24, 2013) (available at http://www.businessweek.com/news/2013-05-23/google-said-to-face-new-antitrust-probe-over-display-ad-market) (discussing Google's 24% market share of the display ad ecosystem and 47% of the U.S. display ad spend in Q1 2013 across all of its display ad services).

104. *See* Press Release, "ANA, 4As Release Statement of Best Practices Addressing Online Piracy and Counterfeiting" (undated) (available at http://www.ana.net/content/show/id/23408).

105. Donna G. Campbell, "Media Matters | Statement of Best Practices to Address Online Piracy and Counterfeiting," Member Bulletin (June 1, 2012) (available at http://www.aaaa.org/news/bulletins/Pages/mmpirate_053112.aspx).

106. *Id.*

107. *Id.*

108. *See* Sandra Aistars, "Best Practices Make Best Partners," Copyright Alliance (May 3, 2012) (available at http://www.copyrightalliance.org/2012/05/best-practices-make-best-partners).

109. Apple, for example, claims that more than 300,000 apps are available through iTunes. News reports cite Apple's apps sales in excess of $4 billion for 2012. Kathleen De Vere, "iOS apps to generate over $4B in 2012 sales, overtake iTunes music—Asymco," Inside Mobile Apps (June 12, 2012) (available at http://www.insidemobileapps.com/2012/06/12/ios-apps-to-generate-over-4b-in-2012-sales-overtake-itunes-music-asymco/).

110. "Trademark Infringement," Google Play (available at https://support.google.com/googleplay/android-developer/answer/141511?hl=en).

111. *Id.*; *see also,* Maty, "Google play store and the supposed trademark infringements," Nenoff (Mar. 29, 2013) (available at http://www.nenoff.com/2013/03/29/google-play-store-and-the-trademark-infringements) (regarding a trademark complaint notification from Google to app developer encouraging him "to resolve this matter with the complainant directly").

112. *Id.*

113. *See* "Apple iTunes Content Dispute Form" (available at http://www.apple.com/legal/itunes/appstorenotices/).

114. *Id.*

115. *See* "Facebook App Center Homepage" (available at http://www.facebook.com/appcenter).

116. *See* "Reporting Trademark Infringements" (available at https://www.facebook.com/help/440684869305015/).

117. *See* "Facebook Online Infringement Complaint Form" (available at http://www.facebook.com/help/contact/?id=208282075858952) (referring to both copyright and trademark infringements); *see* "Reporting Copyright Infringements" (available at https://www.facebook.com/help/400287850027717/).

118. Amazon Press Release, "Introducing Amazon Appstore for Android" (Mar. 22, 2011) (available at http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1541548). The Appstore can be found at http://www.amazon.com/appstore.

119. Amazon Press Release, "Amazon Appstore for Android Celebrates First Birthday with a Week of Deals on Customers' Favorite Apps and Games" (Mar. 15, 2012) (available at http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1673124).

120. *Id.*

121. *See, e.g.*, Amazon's Notice and Procedure for Making Claims of Copyright Infringement (available at http://www.amazon.com/gp/help/customer/display.html/ref=hp_515724_condition?nodeId=508088#copyright).

122. Amazon's Content Guidelines (undated) (available at http://www.amazon.com/gp/help/customer/display.html/ref=hp_left_sib?ie=UTF8&nodeId=15015801).

123. *Id.*

124. *See e.g.*, Rescuecom Corp. v. Google Inc., 562 F3d 123, 129-31 (2d Cir. 2009).

125. *See id.* at 127-130.

126. Rescuecom Press Release, "A Case of David versus Googleiath," (Mar. 5, 2010) (available at https://www.rescuecom.com/a-case-of-david-versus-googleiath.html).

127. "Google AdWords Trademark Policy" (available at https://support.google.com/adwordspolicy/answer/6118?hl=en#).

128. Google Transparency Report, Removal Requests, Copyright (available at http://www.google.com/transparencyreport/removals/copyright/).

129. *Id.*

130. Amit Singhal, "An Update to Our Search Algorithms," *Google's Inside Search Blog* (Aug. 10, 2012) (available at http://insidesearch.blogspot.com/2012/08/an-update-to-our-search-algorithms.html).

131. *Id.*

132. RIAA, "Six Months Later—A Report Card on Google's Demotion of Pirate Sites," *Music Notes Blog* (Feb. 21, 2013) (available at http://76.74.24.142/3CF95E01-3836-E6CD-A470-1C2B89DE9723.pdf).

133. *See, e.g.* RIAA, "One Year, 20 Million Links to Illegal Songs Sent to Google: This Is How It's Supposed to Work?" (May 22, 2013) (available at http://www.riaa.com/blog.php?content_selector=riaa-news-blog&blog_selector=One-Year-&blog_type=&news_month_filter=5&news_year_filter=2013).

134. Google Transparency Report, Removal Requests, Specified Domains (available at http://www.google.com/transparencyreport/removals/copyright/domains/?r=last-year) (last visited June 5, 2013).

135. Alexa, "Where do filestube.com's visitors come from? - Search Traffic" (available at http://www.alexa.com/siteinfo/filestube.com#).

136. *See, e.g.,* "GoDaddy Online Trademark Infringement Complaint Form" (available at https://supportcenter.godaddy.com/DomainServices/TrademarkClaimPage.aspx?prog_id=GoDaddy&isc).

137. *See* "eNom Copyright Policy" (available at http://www.enom.com/terms/copyright_policy.asp).

138. *See* "Filing a Claim with Domains by Proxy" (available at https://www.domainsbyproxy.com/Default.aspx).

139. *See* Michael S. Guntersdorfer, "Practice Tips: Unmasking Private Domain Name Registrations," *Los Angeles Lawyer* (April 2006) (available at http://www.lacba.org/Files/LAL/Vol29No2/2249.pdf).

140. *See* "WhoisGuard Registrant Service Agreement" (available at http://www.whoisguard.com/registrant-agreement.asp); "Domains by Proxy Domain Name Proxy Agreement" (available at https://www.domainsbyproxy.com/policy/ShowDoc.aspx?pageid=domain_nameproxy).

141. *Id.* "Domains by Proxy Domain Name Proxy Agreement" (available at https://www.domainsbyproxy.com/policy/ShowDoc.aspx?pageid=domain_nameproxy).

142. Currently providing services, for example, to PFW Rapidgator.net.

143. *See* Monica, "What To Do About Inaccurate WhoIs Data," Domain Tools Blog (Mar. 29, 2011) (available at http://blog.domaintools.com/2011/03/what-to-do-about-inaccurate-whois-data/).

144. *See, e.g.,* "ICANN Uniform Rapid Response Overview" (available at http://newgtlds.icann.org/en/applicants/urs).

145. *See* ICANN, "New gTLD Agreement" (Feb. 5, 2013) (available at http://www.newgtlds.icann.org/en/.../agb/base-agreement-specs-05feb13-en.pdf).

146. *Id.*

147. *See* "eBay VeRO Program Overview" (available at http://pages.ebay.com/help/tp/vero-rights-owner.html).

148. *See* "eBay's NOCI Form" (available at http://pics.ebay.com/aw/pics/pdf/us/help/community/NOCI1.pdf).

149. *Id.*

150. *See, e.g.*, "eBay's VeRO Program" (available at http://www.tabberone.com/Trademarks/Vero/vero.shtml); *see also* "Fight an eBay VeRO Suspension," Bogus Takedowns (undated) (available at http://www.bogustakedowns.com/).

151. For example, infringers can easily avoid solutions that focus on preventing infringement via a subscriber's connection to the Internet through their ISP by shifting to another Internet access point. *See, e.g.,* Internet Society, "Perspectives on policy responses to online copyright infringement: an evolving policy landscape" (Feb. 20, 2011) (available at http://www.internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape).

Chapter 6

SUMMARY OF CONCLUSIONS

This White Paper outlined various components of potential legislation to remedy the dramatic and harmful impact that PFWs have on U.S. intellectual property rightsholders and the U.S. economy as whole.

The IPL Section supports bipartisan efforts in both chambers of Congress to find a solution to the problem of PFWs, as obtaining jurisdiction over these defendants in civil actions filed in federal courts may be impossible and as the costs to the U.S. economy and rightsholders caused by PFWs continues to climb.

From a practical perspective, a PFW's ability to close down its operations in connection with one domain name and re-establish them under another domain name almost immediately makes enforcement tied to a specific domain name impractical and ineffective. Indeed, the speed with which these PFWs can change domains allows them to evade enforcement.

While legislation often requires refinement, compromise, and a balancing of the various interests involved, the IPL Section believes and supports the general proposition that the enactment of legislation targeting PFWs can be accomplished without compromising legitimate constitutional and public policy concerns.

More specifically, the IPL Section makes the following recommendations to Congress:

- Continue efforts to expeditiously develop and enact more effective laws to deter online piracy and counterfeiting, particularly by PFWs;
- Consult with a broad spectrum of interests within the intellectual property and technology communities to ensure a viable legislative solution is proposed;
- Appropriately balance the interests of, and the respective burdens that would be placed upon, IP rights-holders, Internet businesses, and Internet users;
- Avoid unduly impeding freedom of speech and expression, retarding the future growth of the Internet, or stifling legitimate innovations in the structure or functionality of the Internet;
- Establish new remedies only after taking full account of the impact on the structure or functionality of the Internet and the potential for harm thereto;
- Absent clear justification, neither expand nor contract existing third party copyright liability, or exceptions and limitations on liability under existing trademark and copyright law;
- Ensure that any new legislative proposals comply with existing treaty obligations, particularly those governing the international treatment of intellectual property rights;
- Vest jurisdiction of actions seeking civil or criminal remedies in the United States District Courts;
- Permit the imposition of civil remedies following a judicial determination that online piracy and/or counterfeiting has been undertaken by specifically-identifiable PFWs as well as facilitators of such activities;

- Supplement the following civil remedies (which are already available under U.S. law to redress piracy and/or counterfeiting that occurs within U.S. borders) to redress online piracy and counterfeiting undertaken by PFWs, in cases where the intermediary(y)(ies) in question does not taken action voluntarily:
  (1) injunctions directing financial payment processors to freeze the assets of PFWs and to cease doing business with such websites;
  (2) injunctions preventing online advertisers from paying PFWs or from displaying further ads on those websites;
  (3) injunctions requiring search engines to remove PFWs from paid, sponsored links;
  (4) injunctions requiring website hosts to cease hosting PFWs;
  (5) injunctions permitting the seizure and destruction of counterfeit or pirated goods, or their delivery to rightsholders who are willing to bear the shipping and handling costs;
  (6) injunctions requiring the immediate removal of pirated works and/or content, counterfeit marks, logos, insignia, or trade dress that have been made available, displayed, or otherwise promoted by PFWs; and
  (7) monetary damages in the form of disgorgement of profits of the PFWs achieved as a result of the illegal activity, which shall be paid to the rightsholder from the assets frozen or advertising/sponsored links revenue that had been withheld by the intermediaries, as described in points 1-3 above.
- Develop comprehensive public outreach program(s) to educate the public about recognizing and avoiding pirated works and/or content and counterfeit goods, and about the negative impacts that online piracy and counterfeiting have on the U.S. economy, in an effort to decrease public traffic to PFWs;
- Permit copyright and trademark rightsholders to pursue civil remedies on their own behalf (thus creating a "private right of action");
- Enable the U.S. Government to prosecute criminally and/or undertake civil enforcement of copyright piracy and trademark counterfeiting initiated or induced by PFWs and directed to U.S. end-users/customers;
- Include within any proposed legislation the adequate provision of government resources to ensure effective enforcement of IP rights;
- Encourage and expand adoption of voluntary efforts by Internet businesses based in the U.S. to combat online piracy and counterfeiting undertaken by PFWs, including through the following mechanisms:
  - Streamlining and expediting submission and processing of nonjudicial infringement complains;
  - Implementing online nonjudicial complaint forms and automatic takedown tools; and
  - Developing programs designed to educate Internet users about IP rights and to deter infringing activities;
- Encourage and expand robust and proactive voluntary industry programs to identify and remove infringing content and deny access to counterfeited products and/or disassociate from infringing activity, such as voluntary content filtering by hosting sites and partner website vetting by ad networks and payment processors;

- Encourage wider adoption of voluntary industry initiatives both in the U.S. and around the world, as part of a multi-pronged approach to reduce the harm caused by illegal activities of PFWs.

The IPL Section also considered several additional areas, and has provided substantive research within this White Paper to address those areas, but did not reach any conclusions about potential resolutions in those areas. Nonetheless, the IPL Section recommends that Congress undertake fact-finding through hearings or other public *fora* to consider the following issues and determine the most effective (yet least restrictive with respect to existing U.S. individual rights and existing IP law) solution to include in any legislative proposal:

- Whether additional incentives could be identified or implemented to encourage a broader adoption by U.S.-based Internet businesses of voluntary actions to stem illegal pirating or counterfeiting by PFWs; and
- Whether additional civil or criminal remedies are warranted with respect to any U.S.-based entities that participate in the channel(s) of distribution of pirated copyrighted content or counterfeit goods by PFWs.

The IPL Section trusts that Congress will take the analysis and recommendations presented in this White Paper and give due consideration to crafting legislation that balances the competing interests and finds a way to help U.S. intellectual property rightsholders defend their rights against incursion by PFWs.

Appendix

LEGISLATIVE HISTORY (COICA, PIPA AND SOPA)

I. RESOLUTION TF-01

RESOLVED, that the IPL Section supports efforts to combat Internet-based copyright and trademark infringement by ensuring effective remedies against online infringers, counterfeiters and facilitators of such infringement, including those who operate through the use of non-U.S.-based web sites;

FURTHER RESOLVED, that the IPL Section urges Congress to continue efforts to expeditiously develop and enact more effective laws to deter such online infringement;

FURTHER RESOLVED, that the IPL Section urges Congress to consult with a broad spectrum of interests within the intellectual property and technology communities to ensure a viable legislative solution.

NOW THEREFORE the IPL Section supports the enactment of legislation aimed at deterring Internet-based intellectual property infringement, particularly against foreign web sites primarily engaged in infringement of intellectual property protected under the laws of the United States, and providing adequate governmental resources dedicated to combating such infringement.

II. Background: COICA, PIPA, and SOPA

The Federal Government has been strategizing on ways to fight piracy, and especially online piracy, for years. It is estimated, by various government and private sector experts, that intellectual property thefts cost the U.S. economy over $100 billion per year.[1]

The IPL Section supports bipartisan efforts in both chambers of Congress to find a solution to the problem of online trademark counterfeiting and copyright piracy, particularly by Internet sites registered, owned and/or operated outside of the United States, as obtaining jurisdiction over these defendants in civil actions filed in federal courts may be impossible.

From a practical perspective, a foreign counterfeiter's or pirate's ability to close down its operations in connection with one domain name and re-establish them under another domain name makes enforcement tied to a specific domain name impractical and ineffective. Indeed, the speed with which these counterfeiting or pirating web sites can change domains allows them to evade enforcement.

While legislation often requires refinement, compromise, and a balancing of the various interests involved, we believe and support the general proposition that the enactment of legislation targeting foreign websites engaged primarily in piracy or counterfeiting will further the important goal of reducing online infringement, and can be accomplished without compromising legitimate constitutional and public policy concerns.

Given the dramatic edits and public discussions we have seen in recent weeks to in various versions of the bills currently proposed, we fully expect the bills to continue to evolve. The

summaries provided below of the bills as they currently exist (as of Jan. 19, 2012), are provided for the purposes of helping Council members to catch up on the most recent developments in this debate.

A. Senate Action: COICA, the PROTECT IP Act and the OPEN Act

In response to this growing issue of online piracy, a group of Senators, including Judiciary Committee Chairman Patrick Leahy (D-VT), and Orrin Hatch (R-UT) introduced the **Combating Online Infringement and Counterfeits Act ("COICA"),** S. 3804, 111th Cong.. The bipartisan bill focused on combating online infringement and counterfeits. The Senate Judiciary Committee considered the bill during a markup on November 18, 2010 and adopted an amendment in the nature of a substitute. The Committee then reported the bill, as amended, by a unanimous vote of 19-0. The Committee report to accompany the bill was filed December 17, 2010. S. Rep. No. 111-373 (2010). S. 3084 was not considered by the full Senate before the 111th Congress concluded on December 31, 2010.

The COICA legislation, as amended, would have provided the Department of Justice ("DOJ") with additional legal tools necessary to shut down infringing online websites (so-called "rogue" websites). The DOJ would have had the authority to file an *in rem* civil action against the domain name of a site that is "dedicated" to infringing activities, and to obtain an order requiring the US-based domain name registry of such a name to take it offline. In the case of sites associated with domain names registered wholly outside the United States, DOJ could also have obtained orders to prevent ISPs, credit card companies or advertising networks from processing transactions with these websites. COICA included safeguards for domain name owners or site operators to object to such orders.[2] COICA did not provide a private right of action to rightsholders to enable them to enforce their own rights against these types of infringers.

S. 3084 expired at the conclusion of the 111th Congress, and therefore successor legislation would have to be introduced for further congressional consideration of online piracy. On February 16, 2011, the Senate Judiciary Committee held a public hearing entitled, "Targeting Websites Dedicated to Stealing American IP," in order to consider the introduction of a new version of COICA in the 112th Congress. The following witnesses testified: Tom Adams (President and CEO, Rosetta Stone), Scott Turow (President, Authors Guild), Christine N. Jones (EVP, General Counsel and Corporate Secretary, The Go Daddy Group, Inc.), Thomas M. Dailey (Vice President and Deputy General Counsel, Verizon), and Denise Yee (Senior Trademark Counsel, Visa, Inc.). Representatives for both Google and Yahoo! were invited to attend, but declined to appear. At the end of the hearing, Senator Leahy announced that he planned to introduce a revised version of CIOCA during the current Congressional term.

On May 12, 2011, Senator Leahy introduced the **"Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" (the "PROTECT IP Act" or "PIPA") (S. 968)**. Senators Hatch (R-UT), Grassley (R-IA), Schumer (D-NY), Feinstein (D-CA), Whitehouse (R-RI), Graham (R-SC), Kohl (D-WI), Coons (D-DE) and Blumenthal (D-CT) co-sponsored the bill. The bill was referred to the Committee on the Judiciary, which held a markup on May 26, 2011 to consider the bill. The Committee approved the bill unanimously.

Among other departures from the original COICA language, the PROTECT IP Act narrowed the definition of Internet sites "dedicated to infringing activities," provided a private right of action to rightsholders harmed by the owners or registrants of Internet sites "dedicated to infringing activities," and limited the powers accorded to the DOJ in bringing actions against domain names "dedicated to infringing activities" to only those domain names which are foreign-based. The bill gained significant bipartisan support, but also has attracted considerable criticism and opposition.

Senator Ron Wyden (D-OR) announced his opposition to taking up the bill in the Senate, and, to date has successfully stalled Senate action.

On July 22, 2011, Sen. Leahy filed the Senate Judiciary Committee's written report on the PROTECT IP Act. S. Rep. No. 112-39 (2011).

Following several months of inactivity on the bill due to Senator Wyden's hold, Senator Harry Reid (D-NV) introduced a "cloture" motion on December 17, 2011 to "bring to a close" the debate on the motion to allow the PROTECT IP Act to be considered on the floor of the Senate. According to the Congressional Record, the cloture vote was originally scheduled for January 24, 2012, beginning at 2:15 pm.[3]

Immediately after the cloture motion was filed, Senator Wyden again expressed his intent to filibuster the bill.[4] On January 12, 2012, Senator Leahy offered to withdraw a provision in the PROTECT IP Act that was criticized for its impact on Domain Name System ("DNS") security.[5] On January 20, 2012, Senator Leahy issued a public statement about the postponing of the vote on the cloture.[6] A new date has not yet been set.

In the meantime, Senator Wyden introduced his own version of an anti-counterfeiting/ anti-piracy bill in the Senate on December 17, 2011,[7] entitled "**Online Protection and Enforcement of Digital Trade Act" (the "OPEN Act"),** S. 2029, 112th Cong. (2011). The bill was co-sponsored by Sen. Maria Cantwell (D-WA) and Sen. Jerry Moran (R-KS). The Senate bill has been referred to the Senate Finance Committee.

Rep. Darrell Issa (R-CA) introduced a companion bill, H.B. 3782, on January 18, 2012.[8] Twenty-five co-sponsors have been identified to date.[9] The House bill has been referred to both the House Committee on Ways and Means and the Committee on the Judiciary.

On a related note, the House Oversight and Government Reform Committee scheduled a hearing on January 18, 2012 entitled "Government Mandated DNS Blocking and Search Takedowns—Will It End the Internet as We Know It?" The hearing has been postponed and a new date has not yet been set.

B. House Action: Stop Online Piracy Act (H.R. 3261)

The House of Representatives Committee on the Judiciary, Subcommittee on Intellectual Property, Competition and the Internet has held two hearings on the topic of enforcing U.S. trademark and copyright rights against illegitimate web sites. The first was held on March 14, 2011 entitled "Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I." Testimony was presented by Maria A. Pallante (Acting Register of Copyrights, U.S. Copyright Office), David Sohn (Senior Policy Counsel, Center for Democracy and Technology (CDT)), Daniel Castro (Senior Analyst, Information Technology and Innovation Foundation (ITIF)) and Frederick Huntsberry (Chief Operating Officer, Paramount Pictures).

The Committee held a second hearing on April 6, 2011. Testimony was presented at this time by Hon. John Morton (Director of the U.S. Immigration and Customs Enforcement); Floyd Abrams (a First Amendment litigation specialist who testified on his own behalf); Kent Walker (Senior Vice President and General Counsel for Google); and Christine Jones (Executive Vice President and General Counsel for the GoDaddy Group).

On October 26, 2011, several members of the House Judiciary Committee, including Chairman Lamar Smith (R-TX), and ranking Democrat John Conyers (D-MI) introduced the Stop Online Piracy Act ("SOPA") (H.R. 3261), a companion bill to S. 968, but with some significant differences

from the Senate bill. In many areas, the House bill borrows from the language and provisions of the PROTECT IP Act. It also proposes different terms and definitions than the Senate bill, and as originally introduced, it required rightsholders to attempt to obtain voluntary cooperation of intermediaries by following the pre-suit notification procedures outlined in the bill before seeking relief in the courts. It emphasizes targeting foreign websites, and provides additional and alternative approaches to enforce U.S. rights against them.

The House Judiciary Committee's Subcommittee on Intellectual Property, Competition and the Internet held a hearing on H.R. 3261 on November 16, 2011.

The full House Committee on the Judiciary met on December 15 and 16, 2011 to consider the bill and proposed amendments. Written transcripts for the markup sessions can be found at the House Committee on the Judiciary's web site.[10] A Manager's Amendment was introduced, which removed pre-suit notification provisions, as well as several other provisions that distinguished this bill from the PROTECT IP Act.

During these markups, myriad amendments were proposed, most of which did not carry. On January 13, 2012, Chairman Smith agreed to remove the DNS blocking provisions of SOPA.[11]

III. Discussion of Legislative Proposals Introduced in the House and Senate

A. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 ("PROTECT IP Act") (S. 968)

1. Introductory Sections

The first two sections offer a short title and definitions for terms used in the PROTECT IP Act. The following are notable provisions:

First, the phrase "domain name" is defined separately from "nondomestic domain name." The former refers to "any alphanumeric designation, which is registered with or assigned by any … domain name registration authority … ." The latter refers to domain names with both a Registry Operator and Registrar that "are not located in the United States." The reach of a particular PROTECT IP Act section differs depending on which term is used.

Second, the phrase "Internet site dedicated to infringing activities" includes two distinct definitions. The first identifies three types of Internet sites: (1) those that have "no significant use other than engaging in, enabling or facilitating" copyright infringement (specifically the rights of reproduction, distribution or public performance); (2) those that permit circumvention of copyright technological protection measures; or (3) those engaged in "sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark." The second generally identifies Internet sites that are "designed, operated … marketed [or] used, primarily as a means for engaging in, enabling, or facilitating," the three activities described above.

Third, the definition section differentiates among three types of Internet intermediaries: (1) "Financial Transaction Providers," a term defined in the Unlawful Internet Gambling Act; (2) "Information Location Tools," a term defined in the Digital Millennium Copyright Act; and (3) "Internet Advertising Services," a term coined in the PROTECT IP Act. There is a fourth type of Internet intermediary identified—but not defined—in the Act, (4) "Operators" of "nonauthoritative domain name system servers."

It may help to think of these four types of Internet intermediaries by way of example. Visa is a "financial transaction provider" because it is a "financial institution" that is "utilized to effect a credit transaction…" 31 U.S.C. § 5362(4) (2012). Google and Yahoo! are "information location

tools" because their search engines may "link[] users to an online location containing infringing material or infringing activity…" 17 U.S.C. § 512 (2012). Pay-per-click advertisers like Sedo and keyword advertisers like Google are "internet advertising services" because they "sell" and "insert … placement of advertisement[s]" that are "rendered in viewable form for any period of time on an Internet site." And domain name registrars, such as GoDaddy, can be "Operators" of "nonauthoritative domain name system servers."

Notably, the reference to "authoritative" versus "nonauthoritative" domain name servers is a technical one, which has been explained by Maria A. Pallante, Register of Copyrights, as follows:

When a consumer tries to reach a website associated with a domain name, the consumer's ISP identifies and contacts the relevant registry associated with the requested domain name, such as VeriSign for ".com" top-level domain names, because the registry controls the root name servers that will direct Internet traffic to the correct website. The registry, in turn, directs the user to an authoritative domain name server, which, in most circumstances, is the registrar of the specific domain name. The registrar then sends the Internet user to the content identified by its customer, the domain name registrant, which is housed on a specific server, identified by an IP address connected with a particular domain name (or group of domain names).[12]

Fourth, the term "qualifying plaintiff" is defined as either the Attorney General ("**AG**") or "an owner of an intellectual property right … harmed by the infringing activities of an Internet site…"

2. Substantive Sections

The third through fifth sections of the PROTECT IP Act contain its most important provisions.

Sections three and four create two independent federal causes of action to address "Internet sites dedicated to infringing activities." The first, under Section 3, may only be brought by the AG. The second, under Section 4, may be brought either by the AG or by the private rightsholder.

Three important differences between Section 3 and Section 4 causes of action are evident:

- First, section three offers standing solely to the AG, whereas section four offers standing to "qualified plaintiffs," including the AG, intellectual property rights owners, or those authorized to enforce such rights, who are harmed by infringing activities of an Internet site.
- Second, section three concerns only "nondomestic domain names" with both a Registry Operator and Registrar that "are not located in the United States," whereas section four concerns all "domain names."
- Third, section three allows the AG to have court orders served on four types of intermediaries, whereas section four only allows "qualified plaintiffs" to have court orders issued to two types of intermediaries. This raises the question, how did operators (registries) and information location tools (search engines) escape accountability when the private rights owner—rather than the AG—is granted an order by the court?

Section five contains two prongs that extend immunity for intermediaries taking voluntary action against Internet sites dedicated to infringing activities.

- The first prong of section five immunizes Financial Transaction Providers and Internet Advertising Services *against monetary damages* for disabling their services "based on credible evidence" that the Internet site is dedicated to infringing activity.
- The second prong of section five immunizes all intermediaries against *all liability* for disabling or refusing services to a site that "endangers public health"—including sites that "offer, sell, dispense, or distribute" controlled or non-controlled prescription medication that is either adulterated, misbranded or regularly offered without a valid prescription.

It appears that this bill does not immunize operators (registries) or information location tools (search engines) for taking voluntary measures against users "based on credible evidence" of infringement.

3. Savings Clauses

Section six contains three savings clauses: providing 1) that this Act will not limit or expand civil or criminal remedies provided by state or federal law for infringing activities on the Internet; 2) that this Act will not expand or diminish vicarious or contributory liability under 17 U.S.C. § 512 (the DMCA); and 3) that nothing in this Act shall serve as a basis for determining liability under 17 U.S.C. § 512 (the DMCA).

4. Future Studies

Section seven prescribes several future studies and publications. First, the AG is required to provide an annual oversight report to the Senate Judiciary Committee on every cause of action filed by the AG, every injunction issued by a court and every proof of service filed under the PROTECT IP Act. The AG must also report on every action against a recalcitrant intermediary, every motion by an intermediary to modify, vacate or suspend a court order and every related cause of action under the PROTECT IP Act.

Second, the Register of Copyright must conduct a study on the burdens on intermediaries of carrying out PROTECT IP Act actions, as well as the need to reimburse the costs to intermediaries of complying with the legislation.

Third, the Government Accountability Office must provide a report on each private cause of action filed pursuant to the PROTECT IP Act by the end of the first year that the bill is enacted into law.

5. Preventing Importation of Counterfeit Products.

In a separate amendment introduced by Senators Leahy and Grassley during the May 26, 2011 markup session, a new Section 8 was added to proscribe the importation of counterfeit products and infringing devices.

The amendment provides that—notwithstanding the criminal penalties contained in 18 U.S.C. § 1905 (2012) for publication of confidential information and trade secrets—the United States Customs and Border Protection (CBP) is authorized to share information and samples of counterfeit materials with the appropriate trademark owner. The CBP is also authorized to share information and samples of materials designed to circumvent copyright technological protection measures with the appropriate copyright owner.

This amendment departs somewhat from the thrust of the PROTECT IP Act, but is nevertheless a very important clarification for intellectual property owners. It is designed to counteract an increasingly conservative practice of the CBP by which it has refused disclosure of suspected counterfeit materials to the appropriate trademark owner claiming potential liability under 18 U.S.C. § 1905 (relating to government disclosure of confidential information and trade secrets belonging to importers and manufacturers).

6. Public Comment in Support/Opposed to The PROTECT IP Act

a) Statements in Support

Immediately following the introduction of the PROTECT IP Act, a number of organizations expressed their public support of its provisions.

For instance, the U.S. Chamber of Commerce's Global Intellectual Property Center praised the bill, explaining: "Rogue sites and their operators contribute nothing to the U.S. economy. They do not innovate, they do not pay taxes, they do not follow safety standards, and they do not follow the law. Today's vote serves as a wakeup call to those who illicitly profit at the expense of American businesses and consumers—the U.S. will not tolerate your careless, reckless, malicious behavior."[13]

Copyright Alliance explained its support of this bill: "The websites targeted by this legislation are draining income from American businesses and misleading consumers with their unregulated, unlicensed and unsafe practices. . . . This bill provides much-needed tools for law enforcement to do its job and we urge the full Senate to consider it in the very near future."[14]

The National Cable & Telecommunications Association issued its press release supporting the bill, stating: "By cracking down on rogue websites that have for too long encouraged the theft of valuable content and intellectual property, the PROTECT IP Act of 2011 sends a strong message that this illicit practice will no longer be tolerated."[15]

A group of entertainment professionals jointly issued a statement in support of the bill.[16] Representing "more than 400,000 entertainment industry workers including craftspeople, actors, technicians, directors, musicians, recording artists and others whose creativity is at the heart of the American entertainment industry," the statement opines,

> "[W]e believe the PROTECT IP Act is critical to efforts to aggressively combat the proliferation of foreign 'rogue websites' that steal US produced content and profit from it by illegally selling it to the American public. **Let us be very clear: online theft is stealing**. It results in thousands of lost jobs and millions of dollars in lost wages for our members. We reject the claims that shutting down illegal sites may somehow impact legitimate commercial websites. **This bill clearly goes after illegal sites; legitimate and law abiding websites are not the target and we would hope that those who advocate against either of these bills are not condoning illegal activity on the Internet any more than they would condone illegal activity in their bank or grocery store.** Today's passage of the PROTECT IP Act is a significant step toward ending the 'looting' of the creative and artistic entertainment works that constitute our members' hard work, and are an invaluable part of our collective cultural heritage." [17]

The groups signing on to this Joint Statement were the American Federation of Musicians (AFM), American Federation of Television and Radio Artists (AFTRA), Directors Guild of America (DGA), International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, Its Territories and Canada (IATSE), International Brotherhood of Teamsters (IBT) and Screen Actors Guild (SAG).[18]

A coalition of entertainment industry organizations supported the bill, specifically stating, "By helping shut down rogue websites that profit from stolen films, television shows, and other counterfeit goods, this legislation will protect wages and benefits for the millions of middle class workers who bring America's creativity to life."[19] Members of the group include the Independent Film & Television Alliance® (IFTA), the National Association of Theatre Owners (NATO), and the Motion Picture Association of America, Inc. (MPAA).[20]

Finally the American Apparel and Footwear Association issued a statement that "[w]hile the current PROTECT IP Act is a significant improvement over previous attempts at legislation to shut down rogue Web sites that sell counterfeit goods, the U.S. apparel and footwear industry believes this bill can be made stronger. We are pleased that language has been included to allow law enforcement the ability to share information with rightsholders."[21]

b) Statements in Opposition

Since the bill was introduced, several organizations have opposed the bill, articulating concerns about interference with the DNS, potentially overbroad application to web sites located in the U.S. and potential restrictions on free speech. The Center for Democracy and Technology (CDT) has issued statements opposing the bill immediately after its introduction. Shortly after the markup was introduced, their opposition remained, but they acknowledged that some improvements had been made in the new version:

CDT has expressed its concern with this approach, and particularly with the portions of the bill that try to use the domain name system (DNS) to control 'rogue websites,' in previous blog posts and congressional testimony. The Committee today made a few modest but generally positive changes, such as improving transparency via annual oversight reports and tightening some language designed to prevent the bill from undermining the crucial copyright liability 'safe harbor' under section 512 of the DMCA. But CDT's core concerns remain.[22]

Similarly, an association of groups wrote a letter to the Judiciary Committee expressing concerns with the bill.[23] The signatories were the American Association of Law Libraries, Association of College and Research Libraries, American Library Association, Association of Research Libraries, Center for Democracy and Technology, Demand Progress, EDUCAUSE, Electronic Frontier Foundation, Human Rights Watch, Rebecca MacKinnon, Bernard Schwartz Senior Fellow, New America Foundation, Public Knowledge, Reporters sans frontières / Reporters Without Borders and Special Libraries Association. While we have not confirmed that each of these organizations continues to oppose the legislation, it is believed that they have not changed their positions. For instance, the American Library Association posted an article on its blog "applauding" the Internet blackout on January 18, 2012, in protest against both the PROTECT IP Act and SOPA.[24]

Google opposed the bill, having actively participated in the January 18, 2012 blackout protesting both the PROTECT IP Act and SOPA. In addition, Google recently stated, "Like many businesses, entrepreneurs and Web users, we oppose these bills because there are smart, targeted ways to shut down foreign rogue websites without asking American companies to censor the Internet."[25]

B. The Stop Online Piracy Act ("SOPA") (H.R. 3261)

1. AG's Right of Action vs. Private Right of Action

SOPA is similar to its Senate counterpart, the PROTECT IP Act in several respects. The bill maintains the private right of action that was introduced by the PROTECT IP Act. Further, SOPA continues to provide immunity for companies that voluntarily take certain measures against rogue websites. Finally, the bill maintained the AG's power to seek injunctive relief against a rogue website.

Among the similarities is the structure provided to sort Internet intermediaries into four categories. For instance, both bills allow the AG to serve a court order enjoining the illegal conduct on four Internet intermediaries, although the bills use different names for some of these intermediaries. The PROTECT IP Act uses the terms (i) operators, (ii) financial transaction providers, (iii) Internet advertising services and (iv) information location tools, while SOPA refers to (i) service providers, (ii) payment network providers, (iii) Internet Advertising Services and (iv) Internet search engines.

In both bills, private IP rightsholders are limited to taking action against two of these types of intermediaries: (i) financial transaction providers (a.k.a. payment network providers) and (ii) Internet advertising services. SOPA also introduces a new concept for defining which sites come under the purview of the Act. Rather than targeting sites "dedicated to infringing activities" (which

is opposed by some public interest groups who believed the definitions set forth in COICA and PROTECT IP Act are too vague), SOPA targets sites "dedicated to the theft of U.S. property." A site is considered dedicated to the theft of U.S. property if it is a U.S.-directed site: (a) that is "primarily designed" to engage in, enable or facilitate criminal intellectual property violations; or, (b) whose operator "is taking, or has taken, deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out" copyright violations or whose operator operates the site to promote or carry out such violations.

SOPA places special emphasis on targeting foreign infringing sites, defined as U.S.-directed sites with U.S. users whose off-shore based operator commits or facilitates the commission of infringements of U.S. copyrights. Section 102 of SOPA empowers the AG with the authority to request a court order against any such foreign infringing site, which would block the infringing site's access to the U.S. market. Service providers and search engines would be required to take "technically feasible" measures to block access to the foreign infringing site, and payment processors and online advertising services may be required to cease providing services to such sites. The bill also allows the Justice Department to target previously seized rogue sites, which reappear under different domain names, simplifying the process of ensuring that such rogue sites are completely shut down.

The bill also amends various sections of the United States Code to enhance criminal penalties and protections relating to copyright infringement and trafficking in counterfeit goods. In addition, the bill adds criminal penalties for felony infringements of the public performance right, similar to the penalties in place for infringements of the reproduction and distribution rights.

2. Savings and Severability Clauses

SOPA includes new savings clauses designed to confirm that this bill does not expand or diminish rights or liabilities already provided under the First Amendment or under Title 17 of the U.S. Code (relating to copyrights). No such savings clause relating to trademark rights and/or liabilities appears in this bill.

This section also contains a severability clause (Section 2(b)), providing that if any provision of this bill or its application is held to be unconstitutional, the remaining "provisions or applications of the provision to other persons or circumstances shall not be affected thereby."

The Manager's Amendment offered[26] on December 15, 2011 adds three additional savings clauses: 1) confirms that Title I shall not be construed to impose a duty to monitor by ISPs; 2) confirms that Title I shall not be construed to impose a duty on ISPs to design network, technology or service to prevent violations of this bill or to use a specific technology; and 3) confirms that Title I shall not be construed to authorize a court to require any action by the ISP that would "impair the security or integrity of the domain name system."

3. Future Studies

Section 106 prescribes the undertaking of two studies: The first must be undertaken by the Register of Copyrights about the enforcement and effectiveness of this title, and any need for amendments to adapt to emerging technologies. This report must be submitted to Congress within two years of the enactment of the bill.

The second study shall be performed by the Secretary of Commerce within one year of enactment to report on the effectiveness of this bill on the accessibility of "Internet sites dedicated to infringing activity" and the deployment, security and reliability of the domain name system and associated processes such as DNS Security Extensions. This study must also make any recommendations for modifications to this bill.

4. Miscellaneous Provisions

Section 104 of SOPA limits the extent of an intermediary's obligations to comply with a court order under this title. Specifically, an intermediary would only be required to act against the portion of the web site identified in the court order. This section also precludes any civil action from being filed against the intermediary for complying with this act.

Section 105 of SOPA provides immunity for service providers, payment network providers, Internet advertising services, search engines, registries and registrars, for voluntarily blocking access to or ending financial affiliation with an Internet site the intermediary reasonably believes to be a foreign infringing site, or a site dedicated to theft of U.S. property. Such voluntary actions must be within the intermediary's contractual rights.

Section 105 of SOPA also provides similar immunity for intermediaries that voluntarily stop providing, or refuse to provide services to an Internet site "that endangers the public health" by "dealing in "misbranded" or "adulterated" prescription medication. Such action must be taken in good faith and based on credible evidence.

5. Title II: Additional Enhancements to Combat IP Theft

Section 201 of SOPA establishes a new criminal penalty through an amendment to the Copyright Act (17 U.S.C. § 506(a)) for unauthorized willful infringement of certain copyrighted works, *inter alia*, for the "purposes of commercial advantage or private financial gain by the reproduction or distribution . . . including by electronic means." This section provides a number of definitions to describe the offense, including the nature of the willful infringement, the categories of copyrighted works covered, what constitutes a "work prepared for commercial distribution," the threshold economic value for satisfying the offense. The section further provides a rule of construction.

Section 202 of SOPA would amend 18 U.S.C. § 2320(a) in several significant respects. First, it adds a criminal offense for intentionally importing, exporting, or trafficking in counterfeit drugs, or intentionally participating in or knowingly aiding such activity. Second, it increases penalties for violations of 18 U.S.C. § 2320 that knowingly or recklessly cause, or attempt to cause serious bodily harm or death. In the instance of serious bodily harm, current law allows for a maximum penalty for an individual offender of $2,000,000 and 20 years imprisonment. In the instance of death, an individual may additionally face life imprisonment. The bill, if made law, would increase those figures to $5,000,000 and imprisonment for "any term of years or for life," for both serious bodily harm and death.

This section also adds a special category pertaining to "counterfeit military goods or services." The new section would define a special category of such trafficking when the good or service "the use, malfunction or failure of which is likely to cause serious bodily injury or death; disclosure of classified information; impairment of combat operations; or other significant harm to a member of the Armed Forces or national security. The Act further requires that the offender have knowledge that the good or service "is falsely identified as meeting military standards or is intended for use in a military or national security application, or law enforcement or critical infrastructure application." An individual, or "a person other than an individual," convicted under this category would face similarly severe penalties.

Section 203 enhances penalties against individuals and organization for the violation of the existing federal economic espionage act directed at trade secret theft. Section 203 amends 18 U.S.C. § 1831(a) so as to increase penalties for individuals from 15 years to 20 years and increasing the $500,000 to "not less than $1,000,000 and not more than $5,000,000." For offenses

committed by organizations, section 1831(b) of the crimes code is amended to increase the penalty from $10,000,000 to "not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret."

Section 204 of SOPA mandates the coordination of the Intellectual Property Enforcement Coordinator (IPEC), the Secretaries of Treasury and Commerce, the United States Trade Representative, the Chairman of the SEC, and the "heads of other departments and appropriate agencies," in an effort to identify and conduct an analysis of "notorious foreign infringers." This research is to culminate in an IPEC report issued to Congress addressing, primarily:

- Whether NFIs are accessing, or attempting to access U.S. capital markets for funding
- The adequacy of relying on foreign governments to pursue legal action against NFIs
- Policy recommendations to deter NFIs and encourage foreign business to adopt industry norms respecting IP rights

Notably absent from this provision is a definition of "notorious foreign infringers."

Section 205 of SOPA directs the Secretary of State and the Secretary of Commerce, "in consultation with" the Register of Copyrights, to ensure that the protection of U.S. IP rights abroad is a "significant component" of United States foreign and commercial policy. Specifically, 205 mandates the appointment of at least one "intellectual property attaché" assigned to the United States embassy or diplomatic mission in a country in each of six geographic regions specified in the provision (Africa, Europe and Eurasia, East Asia and the Pacific, the Near East, South and Central Asia and the Pacific, and the Western Hemisphere, respectively). These attachés are to be assigned to countries where their presence will likely be most beneficial to the reduction of IP infringement abroad, and are tasked with working with U.S. IP rightsholders and U.S. industry to advance the protection of IP rights in their region of assignment. Additionally, section 205 directs the Intellectual Property Enforcement Coordinator to submit an annual report regarding the activities of all intellectual property attachés serving abroad.

6. Public Comments in Support/Opposed to SOPA

a) Statements in Support

Since SOPA was introduced, the bill has been widely praised in some quarters, and strongly criticized in others. The bill has received strong bipartisan support in the House. Additionally, in a joint statement, the Motion Picture Association of America, Independent Film and Television Alliance, National Association of Theatre Owners and Deluxe applaud the bill's sponsors for "reaching across the aisle to craft balanced IP enforcement legislation that targets rogue websites and illegal streaming."[27] Similarly, U.S. Chamber of Commerce president and CEO Thomas J. Donohue commends the bill's cosponsors for "standing up to mass theft of American intellectual property."[28] The National Music Publishers' Association urges the House to "move this important bill forward soon."[29] The Screen Actors' Guild joined together with the American Federation of Musicians, the American Federation of Television and Radio Artists, Directors' Guild of America, International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, its Territories and Canada, the International Brotherhood of Teamsters and issued a joint statement confirming their support of the bill.

ASOP, the Alliance for Safe Online Pharmacies, announced its support of the bill on October 31.[30] ASOP's members include the American Pharmacists Association, Eli Lilly and Company, LegitScript, Merck, the National Association of Chain Drug Stores, and the Partnership at Drugfree.org.

Appendix

As of December 15, 2011, according to Rep. Lamar Smith in his remarks during the markup of the bill, the following organizations had expressed their support for the bill: "There are about 150 organized supporters of H.R. 3261, and here are some of the groups that support the bill: ABC, the AFL-CIO, American Society of Composers, Authors and Publishers, Americans For Tax Reform, Alliance For Safe Online Pharmacies, Comcast, NBC Universal, Copyright Alliance, Council of Better Business Bureaus, Council of State Governments, ESPN, Major League Baseball and the NFL, Major County Sheriffs, Motion Picture Association of America, National Association of Manufacturers, National Cable and Telecommunications Association, National Center For Victims of Crime, National District Attorneys Association, National Governors Association, National League of Cities, News Corp,, Pfizer, United States Conference of Mayors, United States Chamber of Commerce, Visa and MasterCard."[31]

GoDaddy.com, one of the organizations that testified before the House Committee on the Judiciary and the Senate Judiciary Committee on this topic, apparently confirmed its approval of SOPA in an op-ed article published in *Politico* on October 28, 2011.[32] Since then, in the wake of tremendous protest and termination of services by their customers, GoDaddy has retracted its support of the bill.[33]

Despite mounting public opposition to SOPA, many companies and industry groups still support the bill,[34] arguing that the losses of income to U.S. rightsholders (companies and individuals alike) as a result of concerted counterfeiting and piracy efforts of foreign web sites are simply too great to ignore and a solution must be found to protect innovation in the U.S.[35]

b) Statements in Opposition

Vocal opponents of the PROTECT IP Act have expressed similar concerns with respect to SOPA, stemming from a wide range of issues including how rogue sites are defined in the legislation, what the impact may be on proposed blocking/rerouting Internet traffic, and how it may impact both innovation and free speech. Many of these objections seem to center around the original version of the bill introduced on October 26, 2011, instead of the current version proposed in a Manager's Amendment on November 18. Many of the provisions around which these complaints center have already been removed in the current version of the bill—or are promised to be removed in the subsequent markup of the bill.

Recent objections, including the website blackouts of Jan. 18, 2012, have focused on allegations that the bill calls for censorship.[36] Representative Lamar Smith, Chairman of the House Committee on the Judiciary, has published several explanations of why he is convinced that the bill would not create such a result.[37] However, opposition to the bill on censorship grounds continued.[38] In addition, as a result of the online protests on January 18, eight lawmakers have now withdrawn their support for the SOPA bill.[39]

Google has set up a dedicated forum for expressing its opposition to SOPA, arguing that it would censor the Internet and slow economic growth in the U.S.[40] It supported the protest efforts that occurred on January 18 on myriad web sites, and its "Take Action" page urges visitors to contact their congressmen to voice their opposition to the bill.[41]

Microsoft initially issued a statement in support of both SOPA and PIPA, cautioning that "Safeguards should be included to ensure that rogue sites are identified clearly and appropriately, and that the responsibilities of companies required to take action to ensure compliance are well defined and their liability appropriately limited. In addition, steps should be taken to ensure that the private right of action is not subject to abuse, and that the new actions and resulting orders do not

stifle free speech or the free flow of information."[42] However, as the debate continued, Microsoft reversed its position stating that it opposed the bill as currently drafted.[43]

Opponents also have objected specifically to the DNS blocking provision in SOPA, articulating concerns of potential Internet security risks in addition to the potential for government censorship mentioned above.[44] This provision would mandate DNS filtering and redirection to help identify and block infringing sites. Opponents argue this would not only undermine security protocols without any appreciable impact on anti-piracy efforts, but could ultimately expose consumers to a greater potential cybersecurity threat. On Jan. 13, 2012, Rep. Lamar Smith announced that the DNS blocking provisions would be removed from SOPA as a result of consultations with industry representatives.[45]

David Sohn, Policy Counsel for The Center for Democracy and Technology (CDT), has been quoted as saying that this bill "radically expands" the scope of the PROTECT IP Act, such that "any website that features user-generated content or that enables cloud-based data storage could end up in its cross-hairs." *Id.* Mr. Sohn added that "Payment processors and ad networks would be required to cut off business with any website that rightsholders allege hasn't done enough to police infringement." *Id.*

Opponents have argued that the bill would require ISPs to block non-infringing material that happens to be hosted on the same servers as infringing content, in violation of the First Amendment. Some industry and trade organizations, including the Consumer Electronics Association (CEA), the Computer and Communications Industry Association (CCIA) and NetCoalition have published objections to the bill based on the possibility that as worded, it permits a single instance of counterfeiting or infringing to justify the shutdown of the site following a single notice.[46]

Public interest groups have also challenged the bill, arguing principally that the bill would interfere with the domain name system and that by "creating conflicts between DNS servers, it would make you more vulnerable to hackers, identity theft, and cyberattacks," leading to more censorship and increased liability for copyright infringement.[47]

The Obama White House has adopted a policy whereby it provides a public response to citizen petitions that gain more than 25,000 signatures in a 30 day period. In response to a petition opposing SOPA, the White House has issued a statement about what the administration would, and would not, support in a bill of this sort.[48]

Public Knowledge President Gigi Sohn calls the bill "sweeping" and "draconian" and believes "anyone who writes about, or links to, a site suspected of infringement could also become a target of government action."[49] Public Knowledge further finds that the bill is "significantly worse than its Senate cousin" as "it makes fundamental changes to who faces liability for copyright infringement."[50] Opponents contend that the bill would require search engines to be barred from linking to content (infringing or not), on certain websites, and that it will replace traditional secondary liability doctrines with a new and vague "facilitation" standard.[51]

In addition to freedom of speech and due process concerns, which were similarly voiced in relation to PROTECT IP Act, opponents have also raised "human rights" concerns. Electronic Frontier Foundation ("EFF") believes the bill could negatively impact human rights advocates and whistleblowers "who depend on online tools to protect their anonymity and speak out against injustice."[52] Because payment processors would cut off service to such sites, which may be suspected of copyright infringement as a result of its practice of masking IP addresses when downloading copyrighted content, EFF fears that such organizations would lose much of their ability to raise donations online and would be forced to shut down entirely.[53]

C. Online Protection and Enforcement of Digital Trade Act ("OPEN Act" (S. 2029)):

1. Substantive Provisions of the OPEN Act

As currently proposed in the Senate,[54] the OPEN Act (S. 2029) seeks to modify the Tariff Act of 1930 (19 U.S.C. § 1304) by vesting jurisdiction to hear and decide matters of foreign online piracy or counterfeiting in the International Trade Commission (ITC). It adds Section 337A to the Act, entitled "Unfair Trade Practices Relating to Infringement of Copyrights and Trademarks by Certain Internet Sites."

This bill expressly excludes U.S.-based sites from enforcement efforts, and defines "infringing activity" to include only violations of 17 U.S.C. §§ 506, 1201 and 15 U.S.C. § 1116(d).

Under the bill, a U.S. rightsholder who believes that a particular web site violates its rights may submit a complaint to the ITC, which will launch an ITC investigation into the operation of the site. The rightsholder would provide notice of this complaint to the registrant of the domain name. If the ITC determines that the site indeed qualifies as an "Internet site dedicated to infringing activities," it may generate a cease and desist order directing that the site stop its infringing activities.

A cease and desist order under this bill could then be served on financial transaction providers or Internet advertising services. In a dramatic difference between this bill and the PROTECT IP Act or SOPA, search engines and domain name registrars are not covered under this bill.

The ITC will also submit its determination, the record upon which it is based, and any cease and desist order that it generates to the President, who may "disapprove" of the determination and cease and desist order "for policy reasons," causing the order to be terminated.

By definition, this brief excludes from prosecution those web sites that "ha[ve] a practice of expeditiously removing, or disabling access to, material that is claimed to be infringing activity."

The bill also makes provisions for temporary and preliminary cease and desist orders , payment of a bond to "discourage the filing of frivolous petitions." Similar to prior bills, the OPEN Act provides immunity to intermediaries who have acted in compliance with this bill.

In addition, this bill allows Customs and Border Patrol to share information with the holder of a trademark in order to determine whether the goods were imported in violation of 18 U.S.C. § 1905.

Further complicating the analysis is the fact that the OPEN Act has been referred to different the Senate Finance Committee, instead of the Judiciary Committee as the PROTECT IP Act had been. As a result, the public debate may be somewhat bifurcated due to the different considerations required by each committee.

Like the PROTECT IP Act and SOPA, this bill mandates that regulations be promulgated to establish procedures and to provide guidance to the rightsholder, and that a study be performed of the enforcement and effectiveness of this provision. The study must also include an analysis of any modifications that are required to the bill to account for new technology within two years of enactment of this bill. Unlike the PROTECT IP Act and SOPA, this bill mandates that the study must be conducted by the President.

2. Public Comment in Support/Opposed to the OPEN Act

a) Statements in Support

The OPEN Act currently has a significant number of bipartisan supporters, particularly in the House of Representatives following the January 18 protests.[55] Google, Twitter and Facebook have all made public statements in support of the OPEN Act.[56]

The following are common themes across various companies and industry in statements of support of the OPEN Act. For instance, proponents argue that the vesting of initial authority in the ITC to investigate claims is one of the bill's strongest features.[57] For some parties, OPEN may provide more expeditious relief than the court system.[58]

Proponents of the bill also argue that the ITC is regarded as having a less stringent standard for obtaining injunctive relief than the district courts, which must follow *eBay Inc. v. MercExchange LLC*, and its heightened standard for granting injunctive relief.[59] As a result, obtaining relief through an ITC proceeding could be arguably easier to obtain than through a federal court proceeding. Moreover, the bill is structured to allow electronic submission of information and conduct of hearings.[60] Finally, and perhaps most vocally argued, is that the OPEN Act does not impose any obligation that might undermine the DNS system.[61]

b) Statements in Opposition

Opponents of the OPEN Act argue that requiring all investigations and enforcement proceedings to occur in front of the International Trade Commission (ITC) is inappropriate and that jurisdiction should remain in the federal district courts. For example, the Copyright Alliance has argued, "the proposal, which would utilize the International Trade Commission (ITC) as the venue for enforcing copyrights and trademarks online against foreign based rogue websites, does not provide an effective enforcement tool to artists and creators, and would actually create procedural obstacles and excessive cost burdens that would make this an unworkable alternative for independent artists and creators."[62]

Additional concerns articulated about the OPEN Act have been as follows:

- Orders issued by the ITC are subject to nullification by the President for policy grounds.[63]
- Decisions by the ITC have no *res judicata* preclusive effect on parallel district court proceedings, and indeed, may be appealed to federal courts under 19 U.S.C. § 1337(c).[64]
- Before issuing an order under Section 337, the ITC is required to consider the effect of its order on: public health and welfare; competitive conditions in the United States, the production of like or directly competitive articles in the United States, and United States consumers.[65] No comparable requirement exists in litigation in federal district courts.
- The definition of targeted sites has been significantly narrowed.[66] Exclusions under 337A(a)(8)(C) create ambiguity about what is and is not a site dedicated to infringing activity.[67]
- The ITC has not previously dealt with copyright and trademark infringement in the context of the Internet, and may lack the resources and experience to do so effectively.[68] For instance, a recent ITC report summarized the recent proceedings as follows:

During 2010, there were 108 active section 337 investigations and ancillary proceedings, 63 of which were instituted in 2010. Of these 63, 56 were new section 337 investigations and seven were new ancillary proceedings relating to previously concluded investigations. In all but two of the new section 337 institutions in 2010, patent infringement was the only type of unfair act alleged. The two exceptions were one investigation involving alleged copyright, trademark, and patent infringement, and one investigation involving alleged misappropriation of trade secrets as well as patent infringement.[69]

- The ITC is located in Washington, DC, and proceedings may require rightsholders to send counsel to in-person proceedings or hire counsel based in Washington to act on their behalf. For many complainants, these factors may make ITC proceedings impractical.[70]

- Finally, costs to proceed through trial are uncertain.[71] According to one article the average cost of an action through trial at the ITC is $2-3.75 million and takes 15-18 months.[72]

More statements in support and/or statements in opposition were expected appear as the OPEN Act wound its way through the legislative process. Most such comments were expected to focus on the choice of the ITC as the initial forum for redressing complaints about willful online infringement of trademark and copyright interests.

Notes

1. For instance, Chairman Lamar Smith explained that "[t]he theft of America's intellectual property costs the U.S. economy more than $100 billion annually and results in the loss of thousands of American jobs." *Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) (statement of Lamar Smith, Chairman, H. Comm. on the Judiciary) (available at http://judiciary.house.gov/index.cfm/hearings?ContentRecord_id=37AAB337-02A8-575F-17AA-354B02B2B576); *see also* GAO Report on Intellectual Property, "Federal Enforcement Has Generally Increased, but Assessing Performance Could Strengthen Law Enforcement Efforts," at 7 n.1 (2008) (citing a study from the Organization for Economic Cooperation and Development called "The Economic Impact of Counterfeiting and Piracy" which estimated the value of international theft of IP at $200 billion) (available at http://www.gao.gov/new.items/d08157.pdf).

2. S. Rep. No. 111-373 at 8, 12. COICA as originally introduced would have required the Attorney General to publish a listing of domain names suspected of being "dedicated" to infringing activities, but which have not had formal action taken against them. *See* S. 3804, 111th Cong. § 2(j) (as introduced in the Senate Sept. 20, 2010) (section 2(j)(1) stated, "The Attorney General shall maintain a public listing of domain names that, upon information and reasonable belief, the [DOJ] determines are dedicated to infringing activities but for which the Attorney General has not filed an action under this section"). In response to numerous concerns, including from technology advocacy groups, the Amendment removed the section requiring this "Internet blacklist." *See* S. Rep. No. 111-373 (section 2(j) was removed as a result).

3. 157 Cong. Rec. S8783 (daily ed. Dec. 17, 2011) (statement of Sen. Harry Reid) (available at http://www.gpo.gov/fdsys/pkg/CREC-2011-12-17/pdf/CREC-2011-12-17-pt1-PgS8783-7.pdf#page=1).

4. Press Release, "Ron Wyden Senator for Oregon, Wyden Delivers Floor Speech on the Motion to Proceed to Protect IP" (Dec. 17, 2011) ("Therefore, I will be working with colleagues on both sides of the aisle over the next month to explain the basis for this wide-spread concern and I intend to follow through on a commitment that I made more than a year ago, to filibuster this bill when the Senate returns in January.") (available at http://www.wyden.senate.gov/news/press-releases/wyden-delivers-floor-speech-on-the-motion-to-proceed-to-protect-ip). This statement is repeated in the Congressional Record immediately following Sen. Reid's request for scheduling, but the Record incorrectly categorized his statement as relating to the "Personal Information Protection Act" (presumably because Sen. Wyden used the acronym "PIPA" in his remarks). 157 Cong. Rec. S8783 (daily ed. Dec. 17, 2011) (statement of Sen. Ron Wyden) (available at http://thomas.loc.gov/cgi-bin/query/R?r112:FLD001:S08783) (item 7 refers to Personal Information Protection Act, but this is a link to Sen. Wyden's statement about the PROTECT IP Act). Given the duplication between Sen. Wyden's press release (specifically referring to the Protect IP Act) and this statement on the public record, it appears that the Congressional Record simply refers to the wrong bill with respect to Sen. Wyden's remarks.

5. Press Release, Patrick Leahy Senator for Vermont, "Comment of Senator Patrick Leahy On Internet Service Providers And The PROTECT IP Act" (Jan. 12, 2012) (available at http://www.leahy.senate.gov/press/press_releases/release/?id=721ddff6-3399-4d56-a966-bca3f848759b); *see also* David Kravetz, "Leahy Offers to Remove Net-Altering DNS Redirects in Anti-Piracy Bill," *Wired Magazine, Threat Level* (Jan. 12, 2012) (available athttp://www.wired.com/threatlevel/2012/01/leahy-pipa-amendment/); Juliana Gruenwald, "Leahy Offers Major Concession On Online Piracy Bill," *National Journal*, Jan. 12, 2012 (available at http://www.nationaljournal.com/tech/leahy-offers-major-concession-on-online-piracy-bill-20120112).

6. Press Release, Patrick Leahy Senator for Vermont, "Comment of Senator Patrick Leahy on Postponement of The Vote on Cloture on the Motion to Proceed to the PROTECT IP Act" (Jan. 20, 2012) (available at http://leahy.senate.gov/press/press_releases/release/?id=467FB8F0-828D-403C-9B7B-8BF42D583C3E).

7. Press Release, Ron Wyden Senator for Oregon, Wyden, Moran, Cantwell Introduce IP Protection Bill that Will Not Break the Net (Dec. 17, 2011) (available at http://www.wyden.senate.gov/news/press-releases/wyden-moran-cantwell-introduce-ip-protection-bill-that-will-not-break-the-net). Senator Wyden released an early draft of his bill to the public on December 8, 2011, in advance of its introduction in the Senate. Press Release,

Ron Wyden Senator for Oregon, Wyden-Issa Release Draft Digital Trade Legislation (Dec. 8, 2011) (available at http://www.wyden.senate.gov/news/press-releases/wyden-issa-release-draft-digital-trade-legislation). The early draft could be found on http://www.keepthewebopen.com/open, where public comments on the specific draft language were solicited and published. . OPEN: Online Protection & Enforcement of Digital Trade Act, From the Office of Congressman Darrell Issa, http://www.keepthewebopen.com/open. The web site remains in operation as of this writing.

8. The full title of the companion bill is the same as the Senate version. See Summary & Status Report for H.R. 3782, http://hdl.loc.gov/loc.uscongress/legislation.112hr3782.

9. *See* Summary & Status Report for H.R. 3782 (available at http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03782:@@@P). The Co-Sponsors are: Rep. Spencer Bachus (R-AL), Rep. John Campbell (R-CA), Rep. Jason Chaffetz (R-UT), Rep. Peter A. DeFazio (D-CA), Rep. Lloyd Doggett (D-TX), Rep. Michael F. Doyle (D-PA), Rep. Keith Ellison (D-MN), Rep. Anna G. Eshoo (D-CA), Rep. Blake Farenthold (R-TX), Rep. Raul M. Grijalva (D-TX), Rep. Alcee L. Hastings (D-FL), Rep. Michael M. Honda (D-CA), Rep. Timothy V. Johnson (R-IL), Rep. James R. Langevin (D-RI), Rep. Zoe Lofgren (D-CA), Rep. Doris O. Matsui (D-CA), Rep. Patrick T. McHenry (R-NC), Rep. George Miller (D-CA), Rep. Jared Polis (D-CO), Rep. Dennis Ross (R-FL), Rep. F. James Sensenbrenner, Jr. (R-WI), Rep. Jackie Speier (D-CA), Rep. Fortney Pete Stark (D-CA), Rep. Mike Thompson (D-CA), and Rep. Lynn C. Woolsey (D-CA).

10. *Full Committee Markup of (Continued): H.R. 3261, the "Stop Online Piracy Act,"* House Committee on the Judiciary (Dec. 16, 2011) (available at http://judiciary.house.gov/index.cfm/hearings?ID=8333081B-F95A-639C-8CBD-B62E28C34382).

11. Press Release, Lamar Smith Congressman for the 21st District of Texas, "Smith to Remove DNS Blocking from SOPA, Retains Strong Provisions to Protect American Technology and Consumers," (Jan. 13, 2012) ("After consultation with industry groups across the country, I feel we should remove Domain Name System blocking from the Stop Online Piracy Act so that the Committee can further examine the issues surrounding this provision. We will continue to look for ways to ensure that foreign websites cannot sell and distribute illegal content to U.S. consumers.") (available at http://judiciary.house.gov/index.cfm/press-releases?ID=1B599847-E075-63F8-612A-C2537551E11B).

12. *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites (Part I & II): Hearing Before the Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary*, 112th Cong. 25 n.10 (2011) (statement of Maria A. Pallante, Acting Register of Copyrights) (available at http://judiciary.house.gov/_files/hearings/printers/112th/112-153_65186.PDF).

13. Press Release, U.S. Chamber of Commerce, "U.S. Chamber Praises Senate Action to Move Forward with PROTECT IP Act" (May 26, 2011) (available at http://www.theglobalipcenter.com/pressreleases/us-chamber-praises-senate-action-move-forward-protect-ip-act).

14. Juliana Gruenwald, "Senate Judiciary Committee Advances Piracy Bill," *National Journal* (May 26, 2011) (available at http://www.nationaljournal.com/tech/senate-judiciary-committee-advances-piracy-bill-20110526).

15. Press Release, National Cable & Telecommunications Association, "Powell Statement Regarding Senate Judiciary Committee Approval of the PROTECT IP Act of 2011" (May 26, 2011) (available at http://www.ncta.com/ReleaseType/MediaRelease/Powell-Statement-Regarding-Senate-Judiciary-Committee-Approval-of-the-PROTECT-IP-Act-of-2011.aspx).

16. Press Release, SAG-AFTRA One Union, "Joint Statement from AFM, AFTRA, DGA, IATSE, IBT and SAG Commending Senate Judiciary Committee Passage of the PROTECT IP Act" (May 26, 2011) (available at http://www.sagaftra.org/joint-statement-afm-aftra-dga-iatse-ibt-and-sag-commending-senate-judiciary-committee-passage-protec).

17. *Id.* (emphasis added).

18. *Id.*.

19. Press Release, Motion Picture Association of America, Inc., America's Creative Community Welcomes Senate Judiciary Committee Passage Of Bill Combating Content Theft" (May 26, 2011) (available at http://www.mpaa.org/resources/ac44d389-df64-4587-9633-16dd17f710d1.pdf).

20. *Id.*

21. Press Release, American Apparel & Footwear Association, "AAFA Welcomes PROTECT IP Act Advancement in Senate," May 26, 2011 (available at https://www.wewear.org/aafa-welcomes-protect-ip-act-advancement-in-senate/).

22. David Sohn, "Copyright Bill Advances, But Draws Plenty of Criticism," Center for Democracy & Technology (May 26, 2011) (available at http://www.cdt.org/blogs/david-sohn/copyright-bill-advances-draws-

plenty-criticism); *see also* David Sohn & Mark Stanley, "The Open Internet Fights Back," Center for Democracy & Technology (Jan. 16, 2012) (available at http://cdt.org/blogs/161open-internet-fights-back).

23. Letter from American Association of Law Libraries, et al., to Sen. Patrick Leahy and Sen. Chuck Grassley, (May 25, 2011) (available at http://www.cdt.org/files/pdfs/20110525_public_interet_968_ltr.pdf) (note that this letter predated the Manager's Amendment to the bill).

24. Corey Williams, "ALA Applauds Internet Blackout in Opposition to PIPA, SOPA," District Dispatch Blog (Jan. 18, 2012) (available at http://www.districtdispatch.org/2012/01/ala-applauds-internet-blackout-in-opposition-to-pipa-sopa/).

25. Django Gold, "Anti-Piracy Bill Threatens Internet, Needs Work: GOP Sens.," *Law360* (Jan. 18, 2012) (available at http://www.law360.com/ip/articles/301071/anti-piracy-bill-threatens-internet-needs-work-gop-sens-).

26. *Full Committee Markup of (Continued): H.R. 3261, the "Stop Online Piracy Act,"* House Committee on the Judiciary (Dec. 16, 2011) (available at http://judiciary.house.gov/index.cfm/hearings?ID=8333081B-F95A-639C-8CBD-B62E28C34382). At the beginning of the House Judiciary Committee markup on December 15, Chairman Smith offered his Manager's Amendment as a complete substitute to SOPA as introduced. That amendment was not voted on before the congressional session ended. On December 15, the Judiciary Committee began a process of debating and voting on amendments to the Amendment in the Nature of a Substitute. A vote on the Amendment in the Nature of a Substitute would not occur until the Committee had considered and voted on all of the "perfecting" amendments to the Substitute. All the amendments that have been considered and that would be considered when the markup resumed were to this text, and not to the bill as originally introduced. The Manager's Amendment therefore has effectively replaced the bill as introduced.

27. Press Release, "Creative Community Hails New Bipartisan House Legislation To Shut Down Rogue Websites That Steal American-Made Content" (Oct. 26, 2011) (available at http://www.mpaa.org/resources/726e1b61-b94b-461a-b4ea-3dc9e7c58452.pdf).

28. Press Release, "U.S. Chamber Praises House Legislation to Protect Jobs and Sever Rogue Websites from the American Marketplace" (Oct. 26, 2011) (available at http://www.uschamber.com/press/releases/2011/october/us-chamber-praises-house-legislation-protect-jobs-and-sever-rogue-websit).

29. Press Release, "House Legislation On Rogue Sites Welcomed By Songwriting And Music Publishing Industry" (Oct. 26, 2011) (available at http://www.nmpa.org/media/showwhatsnew.asp?id=59); *see also* Press Release, "Copyright Industries Release New Ad Supporting Anti-Piracy Legislation" (Dec. 13, 2011) (available at http://www.nmpa.org/media/showrelease.asp?id=207).

30. Press Release, "ASOP Supports U.S. House of Representatives' Effort Targeted at Curbing Illegal Online Drug Sellers and Protecting Public Health" (Oct. 31, 2011) (available at http://www.safeonlinerx.com/2011/11/asop-supports-us-house-of-representatives-effort-targeted-at-curbing-illegal-online-drug-sellers-and.html).

31. Transcript of December 15, 2011 Markup Hearing at 68 (available at http://judiciary.house.gov/_files/hearings/pdf/transcript12152011.pdf).

32. *See* Sandra Aistars, "In Case You Missed it, GoDaddy.com Applauds SOPA," *Copyright Alliance Blog* (Oct. 28, 2011) (available at http://blog.copyrightalliance.org/2011/10/in-case-you-missed-it-godaddy-applauds-sopa/).

33. Daniel Nye Griffiths, "GoDaddy Retracts Support for SOPA," Forbes.com (Dec. 23, 2011) (available at http://www.forbes.com/sites/danielnyegriffiths/2011/12/23/sopa-go-daddy/).

34. *See* Jaikumar Vijayan, "Supporters of SOPA, PIPA stick to their guns; Widespread online protests dismissed as political stunts," *Computer World* (Jan. 18, 2012) (http://www.computerworld.com/s/article/9223525/Supporters_of_SOPA_PIPA_stick_to_their_guns).

35. *See* Opinion, "Brake the Internet Pirates: How to Slow Down Intellectual Property Theft in the Digital Era," *The Wall Street Journal* (Jan. 18, 2012) (available at http://online.wsj.com/article/SB10001424052970203471004577142893718069820.html?mod=WSJ_Opinion_LEADTop&_nocache=1326892507046&user=welcome&mg=id-wsj#printMode) (subscription required); David Carr, "The Danger of an Attack on Piracy Online," *New York Times* (Jan. 1, 2012) (available at http://www.nytimes.com/2012/01/02/business/media/the-danger-of-an-attack-on-piracy-online.html?_r=1).

36. *See, e.g.,* Jenna Wortham, "Protest on Web Uses Shutdown to Take on Two Piracy Bills," *The New York Times* (Jan. 17, 2012) (available at http://www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?_r=1&emc=eta1); Django Gold, "Wikipedia, Google Protest Wavering Anti-Piracy Bills," *Law360* (Jan. 17, 2012) (available at http://www.law360.com/articles/300700/) (subscription required); Catharine Smith & Ramona Emerson, "Mark Zuckerberg: 'Facebook Opposes SOPA And PIPA'", *The*

Huffington Post (Jan. 18, 2012) (available at http://www.huffingtonpost.com/2012/01/18/mark-zuckerberg-sopa_n_1214090.html).

37. *See, e.g.,* "Chairman Smith responds to Wikipedia Publicity Stunt Wikipedia Promotes Fear not Facts," undated (available at http://judiciary.house.gov/issues/issues_RogueWebsites.html as of Jan. 19, 2012); Rep. Lamar Smith, "Letter to the Editor, Lamar Smith Defends SOPA," *Politico*, Dec. 29, 2011 (available at http://www.politico.com/news/stories/1211/70948.html); Rep. Lamar Smith, "Defending SOPA," *National Review Online*, Dec. 1, 2011 (available at http://www.nationalreview.com/articles/284535/defending-sopa-lamar-smith).

38. *E.g.,* Declan McCullough, "How SOPA would affect you: FAQ," *C-Net News,* Jan. 18, 2012 (available at http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/) (provides a list of opponents to the bill that is proposed to be updated and maintained in light of new statements of opposition); Corynne McSherry and Julie Samuels, "Thank You, Internet! And the Fight Continues," *EFF DeepLinks Blog*, Jan. 18, 2012 (available at https://www.eff.org/deeplinks/2012/01/thank-you-internet-and-fight-continues).

39. "Support wanes in US Congress for anti-piracy bill," BBC News, Jan. 19, 2012 (available at http://www.bbc.co.uk/news/world-us-canada-16623831); Eric Engleman and Derek Wallbank, "U.S. Lawmakers Abandon Anti-Piracy Bills as Google Launches Online Protest," Bloomberg News, Jan. 18, 2012 (available at http://www.bloomberg.com/news/2012-01-18/six-u-s-lawmakers-abandon-anti-piracy-bill-support-as-google-protests.html).

40. "Google: End Piracy not Liberty," undated (available at http://www.google.com/takeaction/past-actions/end-piracy-not-liberty/).

41. "More about SOPA and PIPA" (previously available at https://www.google.com/landing/takeaction/sopa-pipa/). Google's three main arguments in opposition to SOPA had been: 1) that it would censor the Internet; 2) that it would kill U.S. jobs; and 3) that it would be completely ineffective—thus not resulting in an end to this type of piracy. *Id.* By the time this White Paper was published, these sites no longer appeared on the Internet; however, the protests they represented had staggering effects. Chenda Ngak, "SOPA and PIPA Internet blackout aftermath, staggering numbers," *CBS News* (Dec. 19, 2012) (available at http://www.cbsnews.com/news/sopa-and-pipa-internet-blackout-aftermath-staggering-numbers/).

42. Dave Burt,"Microsoft Supports Protect IP act, wants to ensure protections for the free flow of information," Microsoft Privacy & Safety (May 26, 2011) (available at http://blogs.technet.com/b/privacyimperative/archive/2011/05/26/microsoft-supports-protect-ip-act-want-to-ensure-protections-for-the-free-flow-of-information.aspx).

43. Dina Bass, "Microsoft Opposes SOPA Piracy Act, Won't Shut Services," *Bloomberg News* (Jan. 17, 2012) (available at http://www.bloomberg.com/news/2012-01-18/microsoft-opposes-proposed-anti-piracy-act-won-t-shut-services.html).

44. Eric Engleman and Chiara Remondini, "Google Plans Home Page Protest Against U.S. Piracy Measures," *Bloomberg Business Week*, Jan. 18, 2012 (available at http://www.businessweek.com/news/2012-01-18/google-plans-home-page-protest-against-u-s-piracy-measures.html); David Lee, "Sopa and Pipa protests not over, says Wikipedia," *BBC News* (Jan. 19, 2012) (available at http://www.bbc.co.uk/news/technology-16628143); "Support wanes in US Congress for anti-piracy bill," *BBC News* (Jan. 19, 2012) (available at http://www.bbc.co.uk/news/world-us-canada-16623831).

45. Greg Sandoval & Declan McCullagh, "DNS provision pulled from SOPA, victory for opponents," *CNET News* (Jan. 13, 2012) (available at http://news.cnet.com/8301-31001_3-57358947-261/dns-provision-pulled-from-sopa-victory-for-opponents/); Press Release, "Smith to Remove DNS Blocking from SOPA" (Jan. 13, 2012) (available at http://judiciary.house.gov/index.cfm/press-releases?ID=1B599847-E075-63F8-612A-C2537551E11B).

46. Jaikumar Vijayan, "Opposition to Stop Online Piracy Act grows," *Computer World* (Oct. 31, 2011) (available at http://www.computerworld.com/s/article/9221339/Opposition_to_Stop_Online_Piracy_Act_grows).

47. Anandashankar Mazumdar and Amy Bivins, "Introduction of House Online Piracy Legislation Sets Off Storm of Controversy," 83 *Pat. Trademark & Copyright J. (BNA)* 5 (Nov. 4, 2011) (referring to statements by the organization, Public Knowledge) (available at http://news.bna.com/ptln/PTLNWB/split_display.adp?fedfid=23322890&vname=ptcjnotallissues&fn=23322890&jd=ptcj_83_5&split=0).

48. In response to two online petitions directed to the White House, the administration issued its statement. *E.g.*, Victoria Espinel (IPEC), Aneesh Chopra, and Howard Schmidt, "Combating Online Piracy while Protecting an Open and Innovative Internet" (available at https://wwws.whitehouse.gov/petitions#!/response/combating-online-piracy-while-protecting-open-and-innovative-internet).

49. Art Brodsky, "Public Knowledge Sees Dangers In New Intellectual Property Bill," Public Knowledge Blog (Oct. 26, 2011) (available at http://www.publicknowledge.org/news-blog/blogs/public-knowledge-sees-dangers-new-intellectual-pro).

50. Sherwin Siy, "House Version of Rogue Websites Bill Adds DMCA Bypass, Penalties for DNS Workarounds," Public Knowledge Blog (Oct. 26, 2011) (commenting on the original version of SOPA introduced in October 2011) (available at http://www.publicknowledge.org/blog/house-version-rogue-websites-bill-adds-dmca-b).

51. *Compare* Nicole Kardell, "Protests Mount Against Proposed Law That Would Cripple the Internet, Crime in the Suites" (Jan. 3, 2012) (available at http://crimeinthesuites.com/tag/first-amendment/) (claiming that search engines bear overwhelming burden from imposition of SOPA and its "facilitation" liability provision); *with* Charlie Osborne, "Google's SOPA press stunt: Can we truly hold them liable?," *ZD-Net iGeneration* (Dec. 30, 2011) (available at http://www.zdnet.com/blog/igeneration/googles-sopa-press-stunt-can-we-truly-hold-them-liable/13971).

52. Trevor Timm, "Proposed Copyright Bill Threatens Whistleblowing and Human Rights," EFF Deeplinks Blog (Nov. 2, 2011) (available at https://www.eff.org/deeplinks/2011/11/proposed-copyright-bill-threatens-whistleblowing-and-human-rights.)

53. *Id.*

54. On January 18, 2012, Representative Issa introduced an identically titled bill in the House, joined by twenty-five co-sponsors.

55. Current statistics show 2 Senators supporting the Senate version (S. 2029) and 25 Representatives co-sponsoring the House version (H.R. 3287), in addition to their initial sponsors.

56. Gautham Nagesh, "Twitter, Facebook, Google endorse alternate online piracy bill" (Jan. 5, 2012) (available at http://thehill.com/blogs/hillicon-valley/technology/202627-twitter-facebook-and-google-endorse-alternate-online-piracy-bill). Others have identified AOL, eBay, Facebook, Google, LinkedIn, Mozilla, twitter, Yahoo!, Zynga, the Consumer Electronics Association (CEA), Computer and Communications Industry Association (CCIA) and netcoalition.com as supporters of the bill. *See* Press Release, "Rep. Mike Thompson Releases Statement Against SOPA, In Support of OPEN Act" (Jan. 18, 2012) (available at http://mikethompson.house.gov/News/DocumentSingle.aspx?DocumentID=275323).

57. *See, e.g.*, Sen. Wyden "The Online Protection and Enforcement of Digital Trade (OPEN) Act," (available at http://wyden.senate.gov/issues/issue/?id=e881b316-5218-4bcd-80a1-9112347fe2f4); Press Release, "Issa Introduces the OPEN Act" (Jan. 18, 2012) (available at http://issa.house.gov/index.php?option=com_content&task=view&id=949&Itemid=28&Itemid=4).

58. Statement of Rep. Zoe Lofgren (D-CA) at 398 (Dec. 15, 2011) ("I would note that the bill that you have authored [the OPEN Act] actually has some due process tests so that you cut off the money, but at least you know that there is an opportunity to be heard even on an expedited basis.") (available at http://judiciary.house.gov/_files/hearings/pdf/transcript12152011.pdf).

59. *See, e.g.* Spansion, Inc. v. Int'l Trade Comm'n, 629 F.3d 1331, 1359 (Fed. Cir. 2010) (holding that the requirement for obtaining an exclusion order at ITC is less stringent than the requirement for obtaining an injunction in a U.S. district court after a trial for patent infringement).

60. *See, e.g.*, 19 C.F.R. § 201.16(f) (2014) (existing rule providing for electronic service in ITC proceedings).

61. *See e.g.*, Eric Goldman, "The OPEN Act: significantly flawed, but more salvageable than SOPA/PROTECT-IP," *ars technica Law & Disorder Blog* (Dec. 2011) (available at http://arstechnica.com/tech-policy/news/2011/12/the-open-act-significantly-flawed-but-more-salvageable-than-sopaprotect-ip.ars).

62. Amanda Reynolds, "Mythbusting at CES," Copyright Alliance Blog (Jan. 10, 2012) (available at http://blog.copyrightalliance.org/2012/01/mythbusting-at-ces/).

63. OPEN Act, § 337A(e)(4) (2012) ("If the President disapproves of a determination of the Commission for policy reasons and notifies the Commission of that disapproval, the determination and any order issued pursuant to the determination shall cease to have force or effect on the date on which the President notifies the Commission of that disapproval."); Sandra Aistars, "OPEN Act Falls Short for Artists and Creators," Copyright Alliance Blog (Dec. 14, 2011) (available at http://blog.copyrightalliance.org/2011/12/open-act-falls-short-for-artists-and-creators/).

64. *See, e.g.*, *In re Convertible Exerciser Patent Litig.*, 721 F. Supp. 596 (D. Del. 1989), *reh'd denied* (Fed. Cir. 1990); *see* Lannon Mfg. Co., Inc. v. U.S. Int'l Trade Comm'n, 799 F.2d 1572 (Fed. Cir. 1989).

65. 19 C.F.R. § 210.75 (2014) ("Prior to effecting any modification, revocation, or exclusion under this section, the Commission shall consider the effect of such action upon the public health and welfare, competitive conditions in the U.S. economy, the production of like or directly competitive articles in the United States, and U.S. consumers.").

66. Senator Wyden explained, "The OPEN Act takes a much narrower and more targeted approach to combating online infringement than other proposed legislation by targeting only sites "primarily and willfully" engaging in infringement" (available at http://wyden.senate.gov/issues/issue/?id=e881b316-5218-4bcd-80a1-9112347fe2f4).

67. As Chairman Smith explained, "The Wyden-Issa bill [the OPEN Act] narrows the definition of an illegal infringing site to such an extreme that it will be virtually meaningless and nearly impossible to prove." Press Release, "OPEN Act Increases Bureaucracy, Won't Stop IP Theft" (Jan. 19, 2012) (available at http://judiciary.house.gov/news/01192012.html?scp=2&sq=lamar%20smith&st=cse).

68. Mitch Glazier, "A Case For Closing OPEN: ITC, 33 Months Later... ," RIAA's *Music Notes* Blog (Jan. 4, 2012) (available at http://riaa.com/blog.php?content_selector=riaa-news-blog&content_selector=riaa-news-blog&blog_selector=Case-For-Closing-OPEN-&news_month_filter=1&news_year_filter=2012) ("Why in the world would we shift enforcement against these sites from the Department of Justice and others who are well-versed in these issues to the ITC, which focuses on patents and clearly does not operate on the short time frame necessary to be effective? In addition, the remedy traditionally offered by the ITC—an exclusion order to prevent foreign criminals from accessing the US market—is precluded under the OPEN Act."); Eric Engleman & Susan Decker , "Fighting Movie Piracy Seen Likely to Swamp U.S. Trade Agency," *Bloomberg News* (Dec. 7, 2011) (available at http://www.bloomberg.com/news/2011-12-07/fighting-movie-piracy-seen-likely-to-swamp-u-s-trade-agency.html); Holly Lance, "Not So Technical: An Analysis of Federal Circuit Patent Decisions Appealed from the ITC," 17 *Mich. Telecomm. & Tech. L. Rev.* 243 (2010) (available at http://www.mttlr.org/volseventeen/lance.pdf) ("The ITC almost exclusively addresses patent infringement violations, possibly because trademark and copyright holders are able to register their intellectual property with Customs and Border Protections and therefore may not have as much use for the protections of the ITC.").

69. ITC, The Year in Trade 2010, Operation of the Trade Agreements Program, Pub. 4247 at xvii (July 2011) (available at http://www.usitc.gov/publications/332/pub4247.pdf).

70. MPAA Press Release, "OPEN Act Ineffective in Targeting Growing Threat of Foreign Criminal Websites" (Jan. 11, 2012) (available at http://www.mpaa.org/resources/428712e0-704e-4f00-b2ab-2e5c59b35a82.pdf) ("It creates a time consuming and costly method for copyright holders to adjudicate against foreign thieves. Instead of using the federal courts that already decide copyright infringement cases, it adds additional hurdles for independent artists and small businesses. The bill does not contain technical means to block foreign websites from the American market and it allows companies profiting from online piracy to advocate for foreign rogue websites against rightful American copyright holders. Finally, the legislation will lead to a costly expansion of bureaucracy.").

71. Patent litigators Steven Carlson and Alexander Harguth (Fish & Richardson, P.C.) wrote in a presentation about proceedings in the ITC, "Budget will be similar to district court litigation, except that fees and costs will be compressed into one year, instead of spread out over several years." (available at http://www.fr.com/files/uploads/attachments/munich/2-CarlsonAndHarguth-ITC.pdf).

72. Tim Smith & Katherine A. Franco, "Patent Enforcement at the International Trade Commission: Is It Worth It?," *Renewable Energy World*, Feb. 18, 2011 (previously available at http://www.renewableenergyworld.com/rea/news/article/2011/02/patent-issues-patent-enforcement-at-the-international-trade-commission-is-it-worth-it).

About the ABA Section of Intellectual Property Law

From its strength within the American Bar Association, the ABA Section of Intellectual Property Law (ABA-IPL) advances the development and improvement of intellectual property laws and their fair and just administration. The Section furthers the goals of its members by sharing knowledge and balanced insight on the full spectrum of intellectual property law and practice, including patents, trademarks, copyright, industrial design, literary and artistic works, scientific works, and innovation. Providing a forum for rich perspectives and reasoned commentary, ABA-IPL serves as the ABA voice of intellectual property law within the profession, before policy makers, and with the public.