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.

As the Supreme Court has noted, “copyright supplies the economic incentive to create and disseminate ideas,” and “[a] well-functioning international copyright system would likely encourage the dissemination of existing and future works.” 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.” 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 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
Introduction

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. 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. 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. 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. 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.\textsuperscript{11} The World Health Organization (WHO) reports that over 50% of pharmaceuticals sold from sites that conceal their physical address are counterfeit.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.


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.”)


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).

