From Sony to SOPA: The Technology-Content Divide

By John Palfrey, Jonathan Zittrain, Kendra Albert, and Lisa Brem
February 23, 2013

From Sony to SOPA: The Technology-Content Divide

Background Note

> *"There was a time when lawyers were on one side or the other of the technology content divide. Now, the issues are increasingly less black-and-white and more shades of gray. You have competing issues for which good lawyers provide insights on either side."* — Laurence Pulgram, partner, Fenwick & West[i]

Since the invention of the printing press, there has been tension between copyright holders, who seek control over and monetary gain from their creations, and technology builders, who want to invent without worrying how others might use that invention to infringe copyrights. Courts and governments have attempted to balance the interests of these two groups, while simultaneously (at least in democratic societies) protecting technologies that further the dissemination of free speech.

In the United States, each technological breakthrough has been accompanied by a chorus of "product Polyannas" and "content Cassandras,"[1] the former promising a bright future of new products, industries, and free speech channels for end users; the latter raising doomsday predictions of rampant piracy and dire threats to content creators and established industries. A famous cri de coeur was the 1982 testimony of Jack Valenti, president of the Motion Picture Association of America (MPAA), who said that "the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone."[2] But perhaps no new copyright-threatening technology has quite compared with the rapid, world-changing sweep and scope of the Internet and the digital age. For the last twenty years—beginning with *Sony v. Universal Studios*[3] (also known as the "Betamax" case)—U.S. courts, Congress, and the Administration have struggled to keep up with technological change and how it impacts intellectual property rights.

The hot debate between technology and content creators came to a boiling point in October 2011 with the release of the Stop Online Piracy Act. The Act was a lightning rod that attracted extreme reactions from both sides and only served to deepen the divide between them. Lawyers and legislators wrestled with the question: Was there any way to bolster anti-piracy laws without curtailing the freedom to invent?

1984: How Safe is the Sony Safe Harbor?

The Supreme Court's 5-to-4 decision in *Sony*—for good or ill—has been considered the progenitor of the digital era of copyright law. [ii] While some scholars hailed *Sony* as the

[i] As quoted in Amanda Bronstad, "Changing Places; Opening Statements," IP Law and Business, 5:3 (2007). Pulgram represented Napster in its copyright infringement case.

[ii] The case turned on whether Sony could legally manufacture and sell the Sony Betamax, one of the first home video recording devices on the market, and whether home video recording was itself a legal activity. The Betamax not only allowed viewers to play a pre-recorded videotape, it also allowed recording

"'Magna Carta' of both 'product innovation' and the 'technology age,'"[4] others felt that the ruling, which allowed home video recording and the manufacture and sale of home video recorders, unfairly benefitted technology producers at the expense of artists and opened the door to piracy and the file-sharing age. As Christopher Alan Hower noted, "With the ability to decide on what terms they would watch television programming, it is no surprise that many viewers and listeners felt justified participating in unauthorized file-sharing."[5]

According to other legal scholars, the most notable and controversial part of the *Sony* decision was not the outcome itself, but rather how the court arrived there. The court held that Sony's manufacture and sale of the video tape recorder was not in violation of copyright laws as an instrument of secondary liability (i.e. unduly enabling infringement by others), primarily because the Betamax could be shown to have substantial non-infringing uses (also called "dual use").

Edward Lee, in his 2005 paper in the *Journal of Business Ethics*, noted that *Sony* was the "first case ever filed in which copyright holders attempted to stop the manufacture of a technology," and that the Sony doctrine had "constitutional underpinnings, since allowing a copyright holder to bar the sale of technologies with substantial non-infringing uses would be tantamount to giving the copyright holder an exclusive right over the technologies."[6] Lee also pointed out that *Sony* rightly followed traditional secondary liability standards by disallowing a safe harbor for entities engaged in conduct that encouraged infringement, such as "advertising, instructions, or providing a service or the site and facilities for infringement."[7]

Also at issue in *Sony* was the court's decision not to require Sony to employ a reasonably available alternative design (RAD). The plaintiffs argued that Sony should sell the Betamax without the record function or with a safeguard to prevent unauthorized copying. Such RAD arguments have proliferated in the years since *Sony*. However, as Lee noted, "given their own self-interest, copyright holders are poor evaluators of technological development. Indeed, had copyright holders been in control of technological design, the printing press, piano roll, radio, tape recorder, copy machine, cable television, computer, Internet, and a host of other technologies would have never been developed in their original design, if at all."[8]

The dissenting judges in the *Sony* decision held that Sony was liable for infringement because time shifting, in which users taped television shows to watch at a more convenient time, did infringe on copyrighted works and failed the fair use balancing test.[9]

Regardless of one's opinion of it, *Sony* spawned decades of controversy, resulting in disparate court decisions and a parade of new laws and regulations attempting to clarify the issue of secondary liability in copyright infringement.

---

of up to two hours of television programming. Many viewers used this technology to "time shift"—record a television show or movie in order to watch it at a more convenient time.

1985–1998: All Roads Lead to the DMCA

After its setback in *Sony*, the entertainment industry fought back on several fronts. It successfully excluded sound recording from the first-sale doctrine and banned rental of sound recordings except in nonprofit libraries. The industry was unsuccessful, however, in imposing a royalty on home recording equipment and blank tapes. The recording industry's pleas for such levies fell on deaf ears in Congress, since the industry was earning substantial profits in 1985 from the sale of prerecorded videotapes and, later, from compact discs.[10]

The next major copyright legislation was the Audio Home Recording Act (AHRA) of 1992, a "worldwide accord between record companies and hardware manufacturers,"[11] which Congress created in response to Digital Audio Tape (DAT) technology. DATs were similar to analog cassette recorders and players, except DAT copies were as good as originals. In a departure from *Sony*, the AHRA banned dual-use devices that did not have safeguards against infringement, as well as devices that could produce copies of copies if the content were tagged not-to-be-copied. It also added levies that flowed to copyright holders.[12]

The AHRA's framework for what constituted copies of digital music effectively shaped the next generation of digital music devices, such as the Diamond Rio and iPod MP3 players. In *Recording Industry Association of America (RIAA) v. Diamond Multimedia Systems*, the court found that MP3 transfers were not considered digital audio recordings, which meant that manufacturers of MP3 players did not need to pay royalties, but that such copies were within the definition of personal use, and as such, were permitted under the law.[13]

But even as law makers and courts attempted to modernize copyright law in light of existing technology, the ground shifted fundamentally and irrevocably with the advent of the Internet. Copyright holders understood the need to offer their works for sale in this new distribution channel and turned to encryption and digital rights management to control unauthorized copying. They worried that hackers would circumvent these systems and pressed Congress to enact legislation to protect their interests. Those on the other side of the debate expressed concerns "about the chilling effect of such an expansion of copyright law upon those who transmit content and wish to make fair use of copyrighted works."[14] In 1998, Congress responded by passing a compromise: the Digital Millennium Copyright Act (DMCA).[15]

The DMCA had a two-pronged approach: Title I responded to concerns of copyright holders, while Title II responded to concerns of technology providers and end users. Title I created criminal penalties for both the act of circumventing copyright security measures and the "manufacture, importation, trafficking in, and marketing of devices" that were primarily designed, produced, and marketed for the purpose of circumvention. Examples of circumvention tools made illegal under Title I of the DMCA included DVD-cracking software that removed access controls, such as Handbrake or DeCSS.[16]

Title II, or the Online Copyright Infringement Liability Limitation Act (OCILLA), created safe harbors for Internet infrastructure companies that limited liability for secondary copyright infringement.[iii] The safe harbors harkened back to existing vicarious liability laws by stating that Online Service Providers (OSPs) could only take advantage of the safe harbor if they did not receive financial benefit from the infringing activity and if the OSP had the "right and ability to control such activity." Similarly, the law followed the tenets of contributory liability by stating that OSPs would not be immune if they had knowledge of the infringing material or activity.[17] The DMCA named four specific safe harbors in section 512: (a) conduits, (b) caching, (c) hosting, and (d) linking or search engines. The DMCA also developed a process by which copyright holders could give notice to service providers that hosted or linked to infringing materials:

> The protection from liability available under Sections 512(c) and (d) of the DMCA applies only if the service provider responds expeditiously to remove or disable access to material in accordance with the DMCA's notice and takedown provisions. The DMCA shields the service provider from liability upon good faith removal of allegedly infringing material in response to a notice received under the DMCA.[18]

The DMCA in the Courts

Court applications of the DMCA have helped shape the development of the technology sector. The first test of the DMCA was *Universal City Studios v. Corley*, in which the U.S. Second Circuit Court of Appeals upheld an injunction against the distribution of a program that decrypted DVDs. The court found the program to be in direct violation of the DCMA's prohibition of technology that circumvents controls on accessing content.[19]

Other courts have followed this approach. In *321 Studios v. MGM Studios*, the District Court for the Northern District of California upheld the DMCA's constitutionality and held that DVD copying software violated the DMCA.[20] The court came to a similar conclusion in *RealNetworks v. DVD Copy Control Association*, enjoining a digital media company from offering software that allowed users to copy DVDs.[21] These cases, and others like them, have helped shape the contours of the DMCA anti-circumvention provisions banning media copying tools, though such products remain accessible to users on the Internet.

1999–2005: Whacking the Moles—Napster, Aimster, and Grokster

Before Congress could catch its breath from passing the DMCA, technology—in the form of peer-to-peer (P2P) file sharing—again rendered the current state of the law obsolete. In the beginning of P2P, end users shared files to and from their own personal computers, using the

[iii] Companies covered under the DMCA included Internet Service Providers (ISPs) covered under 512(a) and nearly any other company offering online service under 512 (b), (c), and (d), such as content hosting sites, payment processors, and search engines.

central servers of the service provider to search and index files. Napster was the first and most famous file sharing site. Designed by Shawn Fanning, a 19-year-old Northeastern student, Napster's free program gained momentum virtually overnight. One article explained:

> Aggregating more than 10 million users in the first six month period and attaining a growth rate of 200,000 new subscribers in a single day, Napster became the noisy center of a new social reality that struck terror into even the most sturdy of music entertainment executives. Behind this threatening new reality stands a type of software combining the convergence of mp3 music files with an Internet relay chat feature and an informational website. Coordinated by a couple of central server computers, [Napster] enabled not only community, but also free access to and download of up to 100 million copyrighted songs archived on the private hard drives of up to 100 million subscribers worldwide.[22]

The RIAA filed suit against Napster for copyright infringement. By 2001, the Ninth Circuit found Napster to be secondarily liable, in part because it used its centralized servers to locate files for illegal copying.[23]

The next case in the entertainment industry crosshairs, *Aimster,* occurred two years later. Aimster's system, which allowed America Online chat room users to swap files while in the chat room, was also found secondarily liable.[24] The Seventh Circuit found "Aimster's 'willful blindness' regarding the sharing of infringing material in its chat rooms as tantamount to guilty knowledge."[25] But the Ninth Circuit came to a different conclusion in *Grokster*, finding that Grokster's service,[iv] because of its decentralized nature and substantial non-infringing uses, did qualify for the Sony safe harbor.[26] This "disparity…set the stage for the Supreme Court to revisit the question of indirect liability under the Copyright Act of 1976 for the first time since Sony."[27]

This decision set off a new round of debates about the merits of the initial *Sony* test in light of the technological changes since the 1980s. Scholars like Randal C. Picker, from the University of Chicago, pointed out that a reasonably available alternative design no longer had to be introduced at the beginning of a production run, since most applications could prevent infringing use as the product evolved. Companies could be required by law to push updates to their product that would eliminate infringing uses as they cropped up, similar to Windows Update or software patches.[28]

[iv] Grokster and similar "second-generation" file-sharing services allowed users to connect directly with each other, eliminating the centralized servers that rendered Napster's service illegal. David McGuire, "At a Glance: MGM v. Grokster," *Washington Post*, March 28, 2005, accessed April 15,2013, http://www.washingtonpost.com/wp-srv/technology/articles/groksterprimer_033805.htm.

Other scholars, known as "copyfighters," warned against direct or indirect government regulation that placed ongoing responsibilities on software companies to police technologies. This, they argued, would in effect turn every product into a service and place an unfair burden on these companies. Jonathan Zittrain added that "[G]atekeeping responsibilities might not stop at a software author's own products. [Operating system] makers could be asked to become gatekeepers for applications running on their systems."[29]

The Supreme Court overturned the lower court's decision and found Grokster secondarily liable, based on the fact that "the defendants had actively induced third parties to engage in infringing conduct."[30] This case restricted the scope of the *Sony* safe harbor: even software capable of non-infringing uses could result in liability if the defendant actively induced copyright infringement.

The *Grokster* decision left innovators in a state of legal uncertainty, providing only vague guidelines as to what constituted inducement. The blogosphere buzzed with cries that *Grokster* "chilled innovation."[31] Larry Lessig reacted:

> By making [the development of new technology] a process that goes through the courts, you've just increased the legal uncertainty around innovation substantially and created great opportunities to defeat legitimate competition. You've shifted an enormous amount of power to those who oppose new types of competitive technologies. Even if in the end, you as the innovator are right, you still spent your money on lawyers instead of on marketing or a new technology.[32]

As the courts wrestled with Napster, Aimster, and Grokster, copyright holders tested the idea of applying pressure further upstream in the Internet ecosystem. File sharing sites started to move their bases offshore to avoid copyright laws, and copyright holders sought to attack the links in the chain that were still within reach: U.S.-based telecommunication companies and ISPs. One of the earliest such attempts was a 2002 case involving Listen4Ever, a Chinese music swapping service. In *Arista Records v. AT&T Broadband*, the record companies targeted not Listen4Ever itself, but rather American Internet ISPs, seeking an injunction under the DMCA for them to block access by their subscribers to Listen4Ever. However, Listen4Ever shut down just days after the suit was filed—the suit was abandoned and remained a prosecutorial outlier. Part of the reason could have been the fact that, in some cases, major record labels were in the same corporate family as the targeted ISPs.[33]

File Sharing Evolves: Torrents, Streaming and Harm

After the whack-a-mole games of the early 2000s, online file sharing split into two distinct directions, both facilitated by higher Internet speeds and increasing bandwidth. The first direction was torrent technology; the second was data streaming.

Torrent Technology

BitTorrent, which refers to both a file protocol and a company, was invented as a way to swap GNU/Linux[v] software distributions online without bottlenecks on one server—a legally uncontroversial use, since GNU/Linux is free software. More powerful and faster than the technology that enabled Grokster, torrenting took off as a means of distributing any large file quickly—including music and movies.[34] Although Napster was peer-to-peer in the sense that it facilitated file transfers from one sharer to another, it still required transfers be arranged by its central server, and thus Napster desktop software required some access to Napster's server to work. BitTorrent had no central servers—and, as an open protocol, no control over its users. BitTorrent desktop applications could be used without a visit to BitTorrent.com.

To share a file on the BitTorrent protocol, users first created a "seed," a small file that contained information—"metadata"—about the underlying large file to be shared. In the original protocol, the seed also contained information about a tracker server, a "matchmaker" of sorts that connected users who had the file ("seeders") with people who wanted to download the file ("leechers").[35] After the seed file was posted, users with partial copies shared the files they already had with new downloaders. In fact, they were compelled to do so: in order to download at good bandwidth from fellow file owners, the BitTorrent protocol anticipated that users contemporaneously shared their downloads with others.

Thus, instead of one or two file owners transferring an entire file to those who wanted it, anyone with part of the file typically begins "seeding," speeding up the rate of downloads and eliminating high bandwidth costs for initial hosters. The more demand for a file, the more supply.

The torrent file-sharing ecosystem had a number of different players: torrent client software, which allowed users to resolve torrent files and download content; search engines, which allowed users to find torrents of files that they wanted; and trackers, which provided the matchmaking service for specific torrent files.[36] The motives of these players varied widely. Many of the software producers were for-profit companies, some of which served advertising within their products, but other clients were open source projects that depended on users for product development. Trackers, in contrast, were primarily run by individuals who wanted to provide better access to content (whether it was infringing or not).

From 2002, when such technology was invented, to 2005, when *Wired* published its seminal article on torrent technology, "The BitTorrent Effect," torrent-based P2P sharing took up the part of the file-sharing market that had been filled by companies like Napster, Grokster, and Kazaa.[37] BitTorrent escaped the earlier lawsuits because the file format did have substantial non infringing use, from distributing Linux files to mass downloading software patches for *World of Warcraft*.[38] Instead, content providers often targeted BitTorrent tracker sites, including Oink, SuprNova and BTJunkie, or torrent search engines, such as The Pirate Bay or ISOHunt.[39] Some ISPs also took action to slow file sharing without intervention from media

[v] A popular combination of free operating system software often referred to (erroneously) as Linux.

companies, such as Comcast's traffic shaping initiative that slowed BitTorrent traffic to a crawl. Comcast claimed that P2P traffic slowdowns were a side effect of an effort to create "a better user experience."[40]

But by 2008, there were problems with the "sue the tracker" strategy. Most BitTorrent clients and users had shifted to non-tracker dependent technologies, and search engines that did not run trackers began to proliferate. In 2005, Azureus, an early torrent client, introduced DHT, a format update that allowed for trackerless torrents. Support for DHT was added to most major torrent clients within the next year. Most clients began to use three methods to find peers: DHT, trackers, and PEX (peer exchange). After that, some torrent client software, such as Vuze (the successor to Azureus), began to integrate search into their services, eliminating the need for standalone sites. Search engine websites like the Pirate Bay and EZTV were located outside the United States, and continued to operate despite the criminal convictions of their founders.[41]

By 2011, torrent files themselves became obsolete. Sites and users began switching to magnet links, which eliminated the need for a hosted torrent file. Magnet links, also known as magnet URIs, consisted of unique "hashes" (plain text codes) that identified particular files to torrent. This technology further complicated efforts to legally address P2P file sharing, as torrent search engines no longer needed to host files, instead hosting plain text strings.[42]

Streaming, Cyberlockers, and YouTube v. Viacom

Streaming was the other P2P direction embraced by file-sharing sites and end users. Instead of downloading their own copies of infringing content, users merely streamed from websites as they wanted it. This shift eliminated some of the issues present in earlier file sharing technologies; for example, users could no longer be targeted for re-sharing files since all requests were served by central sites. Most streaming video sites were based on a central search engine (such as YouTube or Veoh) or accessed through external linking sites that organized disparate links to copyrighted content (such as MegaVideo). However, as with Napster, sites that hosted streaming content could be held liable for infringing content, unless they complied with the DMCA safe harbor requirements. YouTube was one of the first sites used for mass streaming and also the first to test the requirements of streaming video hosts to qualify for DMCA provisions. After it was bought by Google for $1.65 billion, a Napster redux ensued.[43] In 2007, entertainment conglomerate Viacom began a long battle against YouTube. Although Google implemented filtering capabilities on YouTube and complied, albeit haphazardly, with takedown requests, Viacom continued its suit, seeking to obtain damages for the years in which Google and YouTube allegedly profited from infringement of Viacom's television shows.

The U.S. Second Circuit Court of Appeals remanded the case to a lower court, concluding that "a reasonable jury could find that YouTube had actual knowledge or awareness of

specific infringing activity on its website."[44] In doing so, the Second Circuit made it clear that the 512(c) safe harbor in the DMCA requires knowledge or awareness of specific infringing activity in order to find a party liable for hosting. On remand, the district court found that YouTube was protected by the safe harbor provision. Viacom had not met its burden of showing that YouTube was aware of specific infringements and that it had influenced or participated in the infringement.[45]

YouTube was certainly not the only headache for copyright holders in the streaming area. Sites like MegaVideo, Veoh, and DailyMotion also hosted copyrighted content, and were occasionally blatant about not removing or encouraging users to post copyrighted content. In addition, another form of site, called a "cyberlocker", emerged. Cyberlockers, such as MegaUpload, served a similar purpose to streaming sites, although they allowed direct downloads of content. Streaming sites and cyberlockers were often easier targets for shutdown or lawsuits than BitTorrent-related sites because they were more likely to host content directly and serve advertisements to users. Streaming sites sprung up and shut down quickly; many sites couldn't make enough money to operate, others feared copyright litigation or other legal actions, while still others were shut down as part of the U.S. government crack down on piracy.

Understanding the Problem: File Sharing by the Numbers

Despite the clear changes in technology, consensus could not be reached on the extent of file sharing's impact on content industry profits. The two numbers most often cited by anti-file-sharing advocates were that 750,000 jobs were lost (or not created) due to file sharing, and that file sharing cost the U.S. economy $200 billion to $250 billion annually. As Julian Sanchez said in piece skeptical of industry numbers, "$250 billion is more than the *combined* 2005 gross domestic revenues of the movie, music, software, and video game industries."[46]

According to Sanchez, these numbers date back to a 1996 Congressional debate about the Anti-Counterfeiting Consumer Protection Act, and before that, to an article in *Forbes.* The United States International Trade Commission estimated in 1988 that the cost was $61 billion and 13,774 jobs lost. Of course, these calculations assumed that each file downloaded was the equivalent of a lost sale. Whether this was the correct way of calculating cost to the U.S. economy was highly controversial.[47]

The Institute for Policy Innovation's 2007 report concluded that "each year, copyright piracy from motion pictures, sound recordings, business and entertainment software and video games costs the U.S. economy $58.0 billion in total output, costs American workers 373,375 jobs and $16 billion in earnings, and costs federal, state, and local governments $2.6 billion in tax revenue."[48] However, in 2010, Felix Oberholzer-Gee and Koleman Strumpf released a study that used previous research to estimate that only 20% of recent sales declines in music could be tied to file sharing, but noted that the empirical evidence was mixed.[49] Increases in

single sales, subscription models, and Internet radio could all explain drops in album sales separately from piracy.[50] These measurement disagreements underscored questions about policy interventions; if experts could not agree on how much harm piracy caused, how could policy makers decide what steps to take and what sort of collateral damage would be worth it?

2006-2011: Policy and Enforcement

The PRO-IP Act of 2008 increased funding for IP enforcement and established the Office of the Intellectual Property Enforcement Coordinator (IPEC). The IPEC, along with Federal agencies—including the U.S. Trade Representative (USTR), the Departments of Commerce, Health and Human Services, Homeland Security (DHS), Justice (DOJ), and State—developed a strategic plan to enforce U.S. domestic and foreign intellectual property interests.

President Obama's administration took a strong policy position in support of IPEC's work and recommended changes to existing laws to bolster copyright enforcement. While most of the recommendations dealt with industrial espionage and cases where infringement could lead to death or bodily harm (such as counterfeit drugs), the report, stating that "it is imperative that our laws account for changes in technology used by infringers,"[51] encouraged Congress to "clarify that infringement by streaming, or by means of other similar new technology, is a felony in appropriate circumstances."[vi] [52]

IPEC's February 2011 Annual Report identified a particularly pernicious IP villain: the foreign rogue site. IPEC described the threats presented by foreign sites that offered counterfeit pharmaceutical drugs and the IPEC's plan to enlist Internet infrastructure companies in the battle against such sites:

> On December 14, 2010, the IPEC announced that American Express, eNom, GoDaddy, Google, MasterCard, Microsoft, Network Solutions, Neustar, PayPal, Visa and Yahoo! have agreed to support a non-profit group that will start taking voluntary action against illegal Internet pharmacies. . . . Last fall, the IPEC challenged the private sector to voluntarily address the health and safety issues presented by rogue online pharmacies.[53]

This announcement occurred in the aftermath of the Wikileaks scandal, during which members of Congress succeeded in pressuring PayPal, Amazon Web Services, Tableau Software and EveryDNS to stop providing services to Wikileaks. In light of that successful maneuver, the prospect of targeting intermediaries who provided services to foreign rogue sites suddenly became much more politically tenable.[54]

In its June 2011 report, the IPEC expanded the rogue site definition to include sites offering "counterfeit products and pirated content, both of which are illegal actions which could be

[vi] Senators Klobuchar, Cornyn and Coons introduced this legislation on May 12, 2011.

used to finance other criminal behavior in addition to posing certain safety risks."[55] The report went on to explain:

> The Administration is committed to facilitating practical and efficient voluntary actions by the private sector that take into account protection of legitimate uses of the Internet, privacy rights, and the principles of fair process. Since the release of the [IP] Strategy, we have facilitated and encouraged dialogue among the different private sector Internet intermediaries that contribute to the dynamic nature and functioning of the Internet, including payment processors, search engines, and domain name registrars and registries. These entities can support efforts by rightholders and law enforcement to reduce online infringement in a manner consistent with our commitment to the principles of fair process, freedom of expression and other important public policy objectives. We believe that most companies share the view that providing services to infringing sites is inconsistent with good corporate business practice, and we are beginning to see several companies take the lead in pursuing voluntary cooperative action.[56]

In October 2010, the Office of the United States Trade Representative (USTR) launched a Special 301 Out-of-Cycle Review of Notorious Markets[vii] that culminated with a February 2011 list of "more than 30 Internet and physical markets that exemplify key challenges in the global struggle against piracy and counterfeiting." The USTR went on to urge "the responsible authorities to intensify efforts to combat piracy and counterfeiting in these and similar markets, and to use the information contained in the Notorious Markets List to pursue legal actions where appropriate.[57] (See **Exhibit 1** for the February 2011 Notorious Markets List.)

ICE Seizures

In addition to a call for voluntary cooperation from Internet intermediaries, the U.S. government began a crackdown on infringing sites. Immigration and Customs Enforcement (ICE) began "Operation In Our Sites", a program that used the USTR's Notorious Market list to target "websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise as well as products that threaten public health

[vii] Congress enacted Section 301 as part of the Trade Act of 1974, the principal law authorizing the U.S. government to address unfair trade practices. "Section 301 directs the president to identify countries that are engaging in unfair trade practices, and to take trade actions against those countries to remedy the problem, including sanctions if necessary." IIP Digital, "U.S. Officials Investigating China's Green Technologies Trade," US Embassy.gov, October 19, 2010, http://iipdigital.usembassy.gov/st/english/article/2010/10/20101019164049trebor0.2237055.html#axzz2Q4deuPLN.

and safety."[58] By the end of November 2011, ICE had seized 150 website domain names that were illegally selling and distributing counterfeit merchandise.[59]

SOPA: Censorship or Remedy?

As foreign sites proliferated, particularly in countries that had little or no copyright protection, copyright holders pushed harder for legislation to combat such threats. IPEC's June 2011 one-year anniversary report revealed that it had been "working closely with Congress on efforts to improve enforcement against websites engaged in substantial infringement activity."[60] On May 12 2011, Senator Patrick Leahy (D-VT) introduced the Protect IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA). PIPA, an updated version of the Combating Online Infringements and Counterfeits Act (COICA), sought to give the U.S. government and copyright holders "additional tools to curb access to 'rogue websites dedicated to infringing or counterfeit goods', especially those registered outside the U.S."[61] PIPA allowed the Department of Justice to issue court orders against website entities when individual offenders could not be identified; that court order then could be used to prevent search engines from providing access to such websites and to halt financial and advertising streams to the website. The House released its own version of PIPA, called the Stop Online Piracy Act (SOPA), in October 2011.

As soon as SOPA was released, intellectual property experts and pundits on both sides of the technology-content divide scrambled to make sense of it. Was it the long-awaited clarification of the controversy that began with *Sony*? Was it "an important step towards addressing counterfeiting and piracy online and the websites that steal the intellectual property of hard working Americans,"[62] as stated in IPEC's June 2011 report? Or was it, as the Electronic Frontier Foundation argued, "Internet blacklist legislation" tantamount to censorship?[63] What would SOPA mean to the existing ecosystem of copyright laws?

Exhibit 1: Office of U.S. Trade Representative's Review of Notorious Markets, February 28, 2011

Global piracy and counterfeiting continue to thrive due in part to marketplaces that deal in infringing goods. The Notorious Markets List identifies selected markets, including those on the Internet, which exemplify the problem of marketplaces dealing in infringing goods and helping to sustain global piracy and counterfeiting. These are marketplaces that have been the subject of enforcement action or that may merit further investigation for possible intellectual property rights infringements.

The Notorious Markets List, previously included in the annual Special 301 Report, will now be published separately. This reflects an effort to further expose these markets, and is in response to the Intellectual Property Enforcement Coordinator's 2010 Joint Strategic Plan on Intellectual Property Enforcement.

This document is the result of an Out-of-Cycle Review of Notorious Markets and follows a separate, dedicated request for comments from interested stakeholders which was initiated on October 1, 2010. The Notorious Markets List does not purport to reflect findings of legal violations, nor does it reflect the United States Government's analysis of the general climate of protection and enforcement of intellectual property rights in the countries concerned. That broader analysis of IPR protection and enforcement is contained in the annual Special 301 report, published at the end of April every year.

The list below recognizes markets in which pirated or counterfeit goods are reportedly available, but is by no means an exhaustive listing of all notorious markets around the world. Rather, the list highlights with concern some of the most prominent examples of notorious markets in each of the categories referenced below. The United States urges the responsible authorities to intensify efforts to combat piracy and counterfeiting in these and similar markets, and to use the information contained in the Notorious Markets List to pursue legal action where appropriate.

Pay-per-download
These sites exemplify the problem of online sales of pirated music on a pay-per-download basis.

> Allofmp3 clones: While the Russia-based allofmp3 (formerly the world's largest server-based pirate music website) was shut down in 2007, nearly identical sites have taken its place.

Exhibit 1 (cont.): Office of U.S. Trade Representative's Review of Notorious Markets, February 28, 2011

Linking

These are online services engaged in "deep linking" to allegedly infringing materials, often stored on third-party hosting sites.

Baidu: Baidu recently ranked as the number one most visited site in China, and among the top ten in the world.

B2B and B2C

Business-to-business (B2B) and business-to-consumer (B2C) websites have been cited by industry as offering a wide range of infringing products (such as cigarettes, clothing, manufactured goods, pharmaceutical products and sporting goods) to consumers and businesses while maintaining intellectual property policies that are inconsistent with industry norms.

Taobao: While recognizing that Taobao is making significant efforts to address the availability of infringing goods through its website, it still has a long way to go in order to resolve those problems. Taobao recently ranked in the 15 most visited sites in the world, and in the five most visited sites in China.

BitTorrent indexing

BitTorrent indexing sites can be used for the high speed location and downloading of allegedly infringing materials from other users. The sites identified below illustrate the extent to which some BitTorrent indexing sites have become notorious hubs for infringing activities, even though such sites may also be used for lawful purposes.

ThePirateBay: ThePirateBay recently ranked among the top 100 websites in both global and U.S. traffic, and has been the target of a notable criminal prosecution in Sweden.

IsoHunt: Canada-based IsoHunt, which has been subject of civil litigation in both Canada and the U.S., recently ranked among the top 300 websites in global traffic and among the top 600 in U.S. traffic.

Btjunkie: This site is among the largest and most popular aggregators of public and non-public "torrents," which find and initiate the downloading process for a particular file.

Kickasstorrents: Another popular indexing site, notable for its commercial look and feel.

torrentz.com: This site is a major aggregator of torrents from other BitTorrent sites.

Exhibit 1 (cont.): Office of U.S. Trade Representative's Review of Notorious Markets, February 28, 2011

BitTorrent trackers

BitTorrent tracker sites can also be used for the transfer of allegedly infringing material by directing users to those peers sharing the infringing content. The sites listed below exemplify how some BitTorrent tracking sites have become notorious for infringing activities, even though such sites may also be used for lawful purposes.

Rutracker: Russia-based Rutracker recently ranked among that country's 15 most visited sites, and among the 300 most visited sites in the world.

Demonoid: Ukraine-hosted Demonoid recently ranked among the top 600 websites in global traffic and the top 300 in U.S. traffic.

Publicbt: This site is one of the most popular BitTorrent trackers with over 30 million users worldwide.

openbittorrent: This site ranks among the most widely used BitTorrent trackers in the world.

zamunda: Bulgarian-based zamunda is currently the target of a noteworthy criminal prosecution.

Other web services

Other internet-based services, such as social media sites or cyberlockers, are widely used for lawful purposes. However, some may facilitate unauthorized access to allegedly infringing materials.

vKontakte: The site, which permits users to provide access to allegedly infringing materials, recently ranked among the five most visited sites in Russia and among the 40 most visited sites in the world.

Live sports telecast piracy

Live sports telecast piracy affects amateur and professional sports leagues by making these protected telecasts and broadcasts freely available on the Internet.

TV Ants: This peer-to-peer service, which reportedly operates from China, exemplifies this problem.

Smartphone software

A number of websites are making Smartphone software applications available to the public without compensating rights holders.

Exhibit 1 (cont.): Office of U.S. Trade Representative's Review of Notorious Markets, February 28, 2011

91.com: This site is reportedly responsible for more than half of all downloaded applications in China.

Source: Office of the United States Trade Representative, available at http://www.ustr.gov/webfm_send/2595.

[1] Peter S. Menell and David Nimmer, "Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and Sony's De Facto Demise," *UCLA Law Review* 55 (2007): 143.
[2] Jack Valenti, Testimony before the 97th Congress House Committee on the Judiciary, April 12, 1982, accessed April 15, 2013, http://cryptome.org/hrcw-hear.htm.
[3] 464 U.S. 417 (1984).
[4] Menell and Nimmer, "Legal Realism in Action," 144.
[5] Christopher Alan Hower, "Reviving Fair Use: Why Sony's Expansion of Fair Use Sparked the File-Sharing Craze", *Chicago-Kent Journal of Intellectual Property* 7 (2008): 75.
[6] Edward Lee, "The Ethics of Innovation: p2p Software Developers and Designing Substantial Noninfringing Uses Under the Sony doctrine," *Journal of Business Ethics* 62 (2005): 148.
[7] Ibid., 149.
[8] Ibid.
[9] Hower, "Reviving Fair Use."
[10] Menell and Nimmer, "Legal Realism in Action," 159.
[11] Ibid., 162.
[12] Ibid., 161-63.
[13] "Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc.," *Berkman Center for Internet and Society*, accessed April 15, 2013, http://cyber.law.harvard.edu/property00/MP3/rio.html.
[14] Menell and Nimmer, "Legal Realism in Action," 164.
[15] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).
[16] Digital Media Law Project,"Circumventing Copyright Controls," *Berkman Center for Internet and Society*, last modified May 9, 2008, http://www.citmedialaw.org/legal-guide/circumventing-copyright-controls.
[17] Menell and Nimmer, "Legal Realism in Action," 168.
[18] Electronic Frontier Foundation, "Copyright: Digital Millennium Copyright Act," accessed April 15, 2013, http://ilt.eff.org/index.php/Copyright:_Digital_Millennium_Copyright_Act#Steps_to_Take_upon_Notice_of_Infringement.
[19] 273 F.3d 429 (2d Cir. 2001).
[20] 307 F. Supp. 2d 1085 (N.D. Cal. 2004).
[21] 307 F. Supp. 2d 1085 (N.D. Cal. 2004).
[22] Markus Giesler and Mali Pohlmann, "The Social Form of Napster: Cultivating the Paradox of Consumer Emancipation," *Advances in Consumer Research* 30:1 (2003): 94-100.
[23] Lee, "The Ethics of Innovation," 150.
[24] Menell and Nimmer, "Legal Realism in Action," 179.
[25] Ibid., 183.
[26] Ibid., 185.
[27] Ibid., 179.
[28] Randal C. Picker, "Rewinding Sony: The Evolving Product, Phoning Home and the Duty of Ongoing Design," *SSRN* (2005).
[29] Jonathan Zittrain, *The Future of the Internet and How to Stop It*. (New Haven: Yale University Press, 2009), Chapter 5 and 286, note 101.
[30] Menell and Nimmer, "Legal Realism in Action," 185.
[31] Larry Lessig and Robert Hof, "Ten Years of Chilled Innovation," *BusinessWeek,* June 28, 2005, http://www.businessweek.com/stories/2005-06-28/ten-years-of-chilled-innovation.
[32] Ibid.
[33] Brian Garrity, ISPs: "Next Target in Piracy War," *Billboard*, 114:35 (2002):10.
[34] Clive Thompson, "The BitTorrent Effect," *Wired.com*, 13:1 (2005), accessed April 15, 2013, http://www.wired.com/wired/archive/13.01/bittorrent.html.
[35] For more information see Azureus FAQ page, http://azureus.sourceforce.net/faq.php.

[36] Adam V. Vickers, "Peering Beyond Today's Internet File Sharing Concerns: The Future of BitTorrent Technology," *Tulane Journal of Technology and Intellectual Property* 133 (2006). See also BitTorrent FAQ, http://www.bittorrent.com/help/faq/concepts.
[37] Thompson, "The BitTorrent Effect."
[38] Fred Locklear, "MPAA lawsuits target BitTorrent, eDonkey and Direct Connect networks," *Ars Technica*, December 14th, 2004, accessed April 15, 2013, http://arstechnica.com/old/content/2004/12/4467.ars.
[39] Michal Czerniawski, "Responsibility of BItTorrent Search engines for Copyright Infringements," *SSRN*, accessed April 15, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1540913. See also Jeremy Goldmeier, "Squeals of OiNK lovers Reverberate Across the Internet," *Paste Magazine*, October 24, 2007, accessed April 15, 2013, http://www.pastemagazine.com/articles/2007/10/squeals-of-oink-lovers-reverberate-across-the-inte.html.
[40] Eric Bangeman, "Comcast shooting itself in the foot with traffic shaping explanations," *Ars Technica*, October 24th, 2007, accessed April 15, 2013, http://arstechnica.com/old/content/2007/10/comcast-shooting-itself-in-the-foot-with-traffic-shaping-explanations.ars.
[41] Nate Anderson, "The Pirate Bay Verdict: Guilty, with Jail Time," *Ars Technica*, April 17, 2009, accessed April 15, 2013, http://arstechnica.com/tech-policy/news/2009/04/the-pirate-bay-verdict-guilty-with-jail-time.ars
[42] Greg Hazel and Arvid Norberg, "Extension for Peers to Send Metadata Files," *BitTorrent.org*, , accessed April 15, 2013, http://bittorrent.org/beps/bep_0009.html.
[43] Associated Press, "Google Buys YouTube for $1.65 Billion," *MSNBC Online*, October 10, 2006, accessed April 15, 2013, http://www.msnbc.msn.com/id/15196982/ns/business-us_business/t/google-buys-youtube-billion/.
[44] 676 F.3d 19 (2d Cir. 2012).
[45] Viacom Int'l Inc. v. YouTube, Inc., 07 CIV. 2103 LLS (S.D.N.Y. Apr. 18, 2013).
[46] Julian Sanchez, " 750,000 Lost Jobs? The dodgy digits behind the war on piracy," *Ars Technica*, October 8th, 2008, accessed April 15, 2013, http://arstechnica.com/tech-policy/news/2008/10/dodgy-digits-behind-the-war-on-piracy.ars/.
[47] Ibid.
[48] Stephen E. Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," *Institute for Policy Innovation*, Policy Report 189 (2007), accessed April 15, 2013, http://www.ipi.org/docLib/20120515_CopyrightPiracy.pdf.
[49] Felix Oberholzer-Gee and Koleman Strumpf, "File-Sharing and Copyright," *Innovation Policy and the Economy* 10 (2010), accessed April 15, 2013 http://www.nber.org/chapters/c11764.pdf.
[50] Micheal DeGusta, "The REAL Death of the Music Industry." *Business Insider*, February 18th, 2011, accessed April 15, 2013, http://articles.businessinsider.com/2011-02-18/tech/30052663_1_riaa-music-industry-cd-era.
[51] The White House Office of Management and Budget, "Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations,"(2011): 10, accessed April 15, 2013, http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf.
[52] Ibid.
[53] U.S. Intellectual Property Enforcement Coordinator [IPEC], " Annual Report on Intellectual Property Enforcement," Executive Office of the President of the United States (2010): 28, accessed April 15, 2013, http://www.cybercrime.gov/ipecreport2010.pdf.
[54] Rebekah Heacock, "Intermediary Censorship of Wikileaks on the Rise," *Open Net Initiative*, accessed April 15, 2013, http://opennet.net/blog/2010/12/intermediary-censorship-wikileaks-on-rise.
[55] IPEC, "Joint Strategic Plan One Year Anniversary," Executive Office of the President of the United States (2011): 5, accessed April 15, 2013, http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_anniversary_report.pdf.
[56] Ibid.

[57] Office of the United States Trade Representative, "USTR Announces Results of Special 301 Review of Notorious Markets," February 2011, http://www.ustr.gov/about-us/press-office/press-releases/2011/february/ustr-announces-results-special-301-review-notorio.
[58] National Intellectual Property Rights Coordination Center, "Operation In Our Sites," accessed April 15, 2013, http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf.
[59] U.S. Immigration and Customs Enforcement, "Operation In Our Sites Protects American Online Shoppers…,"last modified November 28, 2011, http://www.ice.gov/news/releases/1111/111128washingtondc.htm.
[60] IPEC, "Anniversary Report," 8.
[61] Wikipedia, s.v. "Protect IP Act," last modified April 8, 2013, http://en.wikipedia.org/wiki/PROTECT_IP_Act.
[62] 2011 U.S. Intellectual Property Enforcement Coordinator Joint Strategic Plan, One Year Anniversary, (June 2011): 8, accessed April 15, 2013, http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_anniversary_report.pdf.
[63] Electronic Frontier Foundation, "SOPA/PIPA: Internet Blacklist Legislation," accessed April 15, 2013, https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill.