Policy paper writing guidelines final.doc

Policy paper ~ Design paper

A policy paper should have most but not always all of these elements:

1. Executive Summary
    a. Summary of key points in paper for high-level decision makers
    b. 2-5 pages double-spaced
    c. Contains enough information for executive to make decision without reading the rest of the report
2. Introduction
    a. Gives background
    b. Introduces problem
    c. States the problem in one or two sentences. This *problem statement* is a key element of a policy paper. If there is not a clear problem, then you don't need a policy.
    d. Causes and / or elements of the problem.
3. Constraints in solving the problem
    a. Technical
    b. Legal
    c. Political (national & international)
    d. Economic
4. Detailed description of proposed solution or solution(s)
5. Detailed description of how the solution will address the problem and other benefits of the proposed solution(s)
6. Plan for implementation of the solution
7. Negative aspects of the proposed solution(s)

8. Comparison to other possible solutions
9. Argument why proposed solution is better than all alternatives and how the benefits outweigh the negatives
10. Conclusion: Next steps and why the overall recommendation is important

Citing Sources

All facts that are not common knowledge and all ideas that are not your own need to be documented. In general, avoid direct quotation. Instead, paraphrase. The general rules for paraphrasing can be found in *The Mayfield Handbook*.

There are a variety of citation styles but they all share the same two part structure, a marker in the text pointing to a full listing, either in in a footnote or in a list of references. Some styles, such as the one you should employ for this paper, use both footnotes and a list of references at the end of the book. Follow the style of the President's Council of Advisors on Science and Technology Spectrum Policy Report. Continuously number footnotes and include a reference list at the end of document (but before any appendices). The report contains excellent examples of footnotes and reference listings for all of the types of documents that you will encounter except for emails and interviews.

Email:
Author J. K.. (year, month day). Subject Line of Email. Type of communication Email address.
Example:
Perelman L. C. (2012, Oct. 10). Citation styles for e-mail. Email. perelman@mit.edu

Interview
Mentor, J.Q. (year, month,day). Type of Communication.
Example:
Obama, B.H. (2012, Nov. 7) Skype Interview.

Stop Online Piracy Act

From Wikipedia, the free encyclopedia

The **Stop Online Piracy Act** (**SOPA**) is a United States bill introduced by U.S. Representative Lamar S. Smith (R-TX) to expand the ability of U.S. law enforcement to fight online trafficking in copyrighted intellectual property and counterfeit goods. Provisions include the requesting of court orders to bar advertising networks and payment facilities from conducting business with infringing websites, and search engines from linking to the websites, and court orders requiring Internet service providers to block access to the websites. The law would expand existing criminal laws to include unauthorized streaming of copyrighted content, imposing a maximum penalty of five years in prison.

what are all the provisions

Stop Online Piracy Act

Full title	"To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes." —H.R. 3261[1]
Acronym	SOPA
Colloquial name(s)	House Bill 3261

Citations

Legislative history

- **Introduced in the House as** H.R. 3261 (http://hdl.loc.gov/loc.uscongress/legislation.112hr3261) **by** Lamar Smith (R-TX) **on** October 26, 2011
- **Committee consideration by:** House Judiciary Committee

Proponents of the legislation state it will protect the intellectual-property market and corresponding industry, jobs and revenue, and is necessary to bolster enforcement of copyright laws, especially against foreign-owned and operated websites. Claiming flaws in present laws that do not cover foreign-owned and operated websites, and citing examples of "active promotion of rogue websites" by U.S. search engines, proponents assert stronger enforcement tools are needed.

no enforcement mechanism

Opponents state the proposed legislation threatens free speech and innovation, and enables law enforcement to block access to entire internet domains due to infringing content posted on a single blog or webpage. They have raised concerns that SOPA would bypass the "safe harbor" protections from liability presently afforded to websites by the Digital Millennium Copyright Act. Library associations have expressed concerns that the legislation's emphasis on stronger copyright enforcement would expose libraries to prosecution. Other opponents state that requiring search engines to delete a domain name could begin a worldwide arms race of unprecedented censorship of the Web and violates the First Amendment.

too broad - not enough fight ability

On January 18, 2012, the English Wikipedia, Reddit, and an estimated 7,000 other smaller websites coordinated a service blackout, to raise awareness. In excess of 160 million people viewed Wikipedia's banner. Other protests against SOPA and PIPA included petition drives, with Google stating it collected over 7 million signatures, boycotts of companies and organizations that support the legislation, and an opposition rally held in New York City.

this did kinda go over board but was very sucessful!

In response to the protest actions, the Recording Industry Association of America (RIAA) stated, "It's a

dangerous and troubling development when the platforms that serve as gateways to information intentionally skew the facts to incite their users and arm them with misinformation", and "it's very difficult to counter the misinformation when the disseminators also own the platform."

Access to websites of several pro-SOPA organizations and companies such as RIAA, CBS.com, and others was impeded or blocked with denial of service attacks which started on January 19. Self-proclaimed members of the "hacktivist" group Anonymous claimed responsibility and stated the attacks were a protest of both SOPA and the United States Department of Justice's shutdown of Megaupload on that same day.[2]

Opponents of the bill have proposed the Online Protection and Enforcement of Digital Trade Act (OPEN) as an alternative.[3][4] On January 20, 2012, House Judiciary Committee Chairman Smith postponed plans to draft the bill: "The committee remains committed to finding a solution to the problem of online piracy that protects American intellectual property and innovation ... The House Judiciary Committee will postpone consideration of the legislation until there is wider agreement on a solution."

Contents

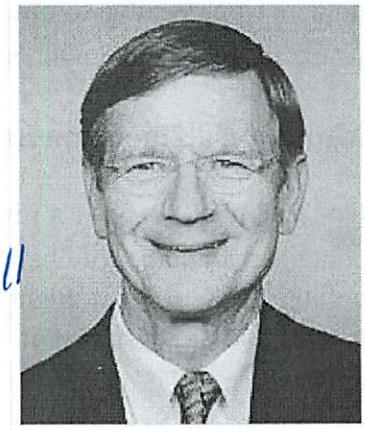
- 1 Overview
  - 1.1 Manager's amendment
- 2 Goals
  - 2.1 Protecting intellectual property of content creators
  - 2.2 Protection against counterfeit drugs
- 3 Impact on online freedom of speech
  - 3.1 Autocratic countries
- 4 Impact on websites
  - 4.1 Websites that host user content
  - 4.2 Weakening of "safe harbor" protections
  - 4.3 Web-related businesses
  - 4.4 Users uploading illegal content
  - 4.5 Internal networks
- 5 Impact on web-browsing software
- 6 Potential effectiveness
- 7 Technical issues
  - 7.1 Deep-packet inspection and privacy
  - 7.2 Domain Name System
  - 7.3 Internet security
  - 7.4 Domain Name System Security Extensions
- 8 Transparency in enforcement
- 9 Supporters
  - 9.1 Legislators
  - 9.2 Companies and organizations
  - 9.3 Others
- 10 White House position
- 11 Opposition
  - 11.1 Legislators
  - 11.2 Companies and organizations
  - 11.3 Others

- 12 International response
- 13 Protest actions
  - 13.1 Wikipedia blackout
  - 13.2 Linked digital attack protest
- 14 Legislative history
  - 14.1 November 16 House Judiciary Committee hearing
  - 14.2 December 15 markup of the bill
    - 14.2.1 Markup outcome
- 15 See also
- 16 References
- 17 External links

Overview

See also: List of legislators who support or oppose SOPA/PIPA

Bill 3261 or H.R. 3261 (http://hdl.loc.gov/loc.uscongress/legislation.112hr3261) , is a proposed law that was introduced in the United States House of Representatives on October 26, 2011, by House Judiciary Committee Chair Representative Lamar S. Smith (R-TX) and a bipartisan group of 12 initial co-sponsors.[5] Presented to the House Judiciary Committee, it builds on the similar PRO-IP Act of 2008 and the corresponding Senate bill, the PROTECT IP Act (PIPA).[6][7]



Rep. Lamar Smith (R-TX) who introduced the SOPA bill.

The originally proposed bill would allow the U.S. Department of Justice, as well as copyright holders, to seek court orders against websites outside U.S. jurisdiction accused of enabling or facilitating copyright infringement. A court order requested by the DOJ could include barring online advertising networks and payment facilitators from conducting business with websites found to infringe on federal criminal intellectual-property laws, barring search engines from linking to such sites, and requiring Internet service providers to block access to such sites.[8][9]

The bill establishes a two-step process for intellectual property-rights holders to seek relief if they have been harmed by a site dedicated to infringement. The rights holder must first notify, in writing, related payment facilitators and ad networks of the identity of the website, who, in turn, must then forward that notification and suspend services to that identified website, unless that site provides a counter notification explaining how it is not in violation. The rights holder can then sue for limited injunctive relief against the site operator, if such a counter notification is provided, or if the payment or advertising services fail to suspend service in the absence of a counter notification.[9]

The second section covers penalties for streaming video and for selling counterfeit drugs, military materials, or consumer goods. The bill would increase penalties and expand copyright offenses to include unauthorized streaming of copyrighted content and other intellectual-property offenses. The bill would criminalize unauthorized streaming of copyrighted content, with a maximum penalty of five years in prison for ten such infringements within six months.[9]

The bill provides immunity from liability to the ad and payment networks that comply with this Act or that take voluntary action to sever ties to such sites. Any copyright holder who knowingly misrepresents that a website is involved in copyright infringement would be liable for damages.[8]

Supporters include the Motion Picture Association of America, pharmaceuticals makers, media businesses, and the United States Chamber of Commerce. They state it protects the intellectual-property market and corresponding industry, jobs and revenue, and is necessary to bolster enforcement of copyright laws, especially against foreign websites.[10] They cite examples such as Google's $500 million settlement with the Department of Justice for its role in a scheme to target U.S. consumers with ads to illegally import prescription drugs from Canadian pharmacies.[11]

Opponents state that it violates the First Amendment,[12] is Internet censorship,[13] will cripple the Internet,[14] and will threaten whistle-blowing and other free speech actions.[12][15]

In October, 2011, co-sponsor Representative Bob Goodlatte (R-VA), chairman of the House Judiciary Committee's Intellectual Property sub-panel, told *The Hill* that SOPA is a rewrite of the Senate's bill that addresses some tech-industry concerns, noting that under the House version of the legislation copyright holders won't be able to directly sue intermediaries such as search engines to block infringing websites and would instead need a court's approval before taking action against third parties.[16]

Manager's amendment

On December 12, 2011 a revised version of the bill was tabled. Titled the "Manager's Amendment", it contained a number of changes in response to criticism of the original.[17] As part of the revisions, the definition of sites that might be subject to enforcement was narrowed: the amendment limited such actions to sites that are designed or operated with the intent to promote copyright infringement, and it now only applies to non-US sites.[18][19][20]

Goals

Protecting intellectual property of content creators

According to Rep. Goodlatte, "Intellectual property is one of America's chief job creators and competitive advantages in the global marketplace, yet American inventors, authors, and entrepreneurs have been forced to stand by and watch as their works are stolen by foreign infringers beyond the reach of current U.S. laws. This legislation will update the laws to ensure that the economic incentives our Framers enshrined in the Constitution over 220 years ago—to encourage new writings, research, products and services— remain effective in the 21st century's global marketplace, which will create more American jobs."[21]

Rights holders see intermediaries—the companies who host, link to, and provide e-commerce around the content—as the only accessible defendants.[22]

Sponsor Rep. John Conyers (D-MI) said, "Millions of American jobs hang in the balance, and our efforts to protect America's intellectual property are critical to our economy's long-term success."[21] Smith added, "The Stop Online Piracy Act helps stop the flow of revenue to rogue websites and ensures that the profits from American innovators go to American innovators."[21]

The Motion Picture Association of America (MPAA) representative who testified before the committee said that the motion picture and film industry supported two million jobs and 95,000 small businesses.[23]

Protection against counterfeit drugs

Pfizer spokesman John Clark testified that patients could not always detect cleverly forged websites selling drugs that were either mis-branded or simply counterfeit.[24]

RxRights, a consumer-advocacy group, issued a statement saying that Clark failed "to acknowledge that there are Canadian and other international pharmacies that do disclose where they are located, require a valid doctor's prescription and sell safe, brand-name medications produced by the same leading manufacturers as prescription medications sold in the U.S."[25] They had earlier said that SOPA "fails to distinguish between counterfeit and genuine pharmacies" and would prevent American patients from ordering their medications from Canadian pharmacies online.[26]

Bill sponsor Smith accused Google of obstructing the bill, citing its $500 million settlement with the DOJ on charges that it allowed ads from Canadian pharmacies, leading to illegal imports of prescription drugs.[11] Shipment of prescription drugs from foreign pharmacies to customers in the US typically violates the Federal Food, Drug and Cosmetic Act and the Controlled Substances Act.[27]

Impact on online freedom of speech

See also: Freedom of speech and Freedom of information

Mentioned on the Texas Insider, President Obama "will not support legislation that reduces freedom of expression", said interviewer Jay Carney.[28]

On *TIME*'s *Techland blog*, Jerry Brito wrote, "Imagine if the U.K. created a blacklist of American newspapers that its courts found violated celebrities' privacy? Or what if France blocked American sites it believed contained hate speech?"[29] Similarly, the Center for Democracy and Technology warned, "If SOPA and PIPA are enacted, the US government must be prepared for other governments to follow suit, in service to whatever social policies they believe are important—whether restricting hate speech, insults to public officials, or political dissent."[30]

Laurence H. Tribe, a Harvard University professor of constitutional law, released an open letter on the web stating that SOPA would "undermine the openness and free exchange of information at the heart of the Internet. And it would violate the First Amendment".[12][31]

The AFL-CIO's Paul Almeida, arguing in favor of SOPA, has stated that free speech was not a relevant consideration, because "Freedom of speech is not the same as lawlessness on the Internet. There is no inconsistency between protecting an open Internet and safeguarding intellectual property. Protecting intellectual property is not the same as censorship; the First Amendment does not protect stealing goods off trucks."[32]

Autocratic countries

According to the Electronic Frontier Foundation, proxy servers, such as those used during the Arab Spring,

can also be used to thwart copyright enforcement and therefore may be regulated by the act.[33]

John Palfrey, co-director of the Berkman Center for Internet & Society, expressed disagreement with the use of his research findings to support SOPA. He wrote that "SOPA would make many [DNS] circumvention tools illegal", which could put "dissident communities" in autocratic countries "at much greater risk than they already are". He added, "The single biggest funder of circumvention tools has been and remains the U.S. government, precisely because of the role the tools play in online activism. It would be highly counter-productive for the U.S. government to both fund and outlaw the same set of tools."[34]

Marvin Ammori has stated the bill might make The Tor Project illegal. Originally sponsored by the US Naval Research Laboratory,[35] the Tor Project creates encryption technology used by dissidents in repressive regimes (that consequently outlaw it). Ammori says that the US Supreme Court case of Lamont v. Postmaster General 381 U.S. 301 (1965) makes it clear that Americans have the First Amendment right to read and listen to such foreign dissident free speech, even if those foreigners themselves lack an equivalent free speech right (for example under their constitution or through Optional Protocols under the United Nations International Covenant on Civil and Political Rights).[36]

Impact on websites

Websites that host user content

Opponents have warned that SOPA would have a negative impact on online communities. Journalist Rebecca MacKinnon argued in an op-ed that making companies liable for users' actions could have a chilling effect on user-generated sites such as YouTube. "The intention is not the same as China's Great Firewall, a nationwide system of Web censorship, but the practical effect could be similar", she says.[37] The Electronic Frontier Foundation (EFF) warned that websites Etsy, Flickr and Vimeo all seemed likely to shut down if the bill becomes law.[38] Policy analysts for New America Foundation say this legislation would enable law enforcement to take down an entire domain due to something posted on a single blog, arguing, "an entire largely innocent online community could be punished for the actions of a tiny minority".[39]

Additional concerns include the impact on common Internet functions such as links from one site to another or accessing data from the cloud. EFF claimed the bill would ban linking to sites deemed offending, even in search results[40] and on services such as Twitter.[41] Christian Dawson, Chief Operating Officer (COO) of Virginia-based hosting company ServInt, predicted that the legislation would lead to many cloud computing and Web hosting services moving out of the US to avoid lawsuits.[42] Even without SOPA, the U.S. Immigration and Customs Enforcement agency (ICE) has already launched extradition proceedings against Richard O'Dwyer in the UK. O'Dwyer hosted the TVShack.net website which had links to material elsewhere and did not host any files. ICE has stated that it intends to pursue websites even if their only connection to the USA is a .com or .net web domain.[43]

The Electronic Frontier Foundation have stated that the requirement that any site must self-police user generated content would impose significant liability costs and explains "why venture capitalists have said en masse they won't invest in online startups if PIPA and SOPA pass".[44]

Proponents of the bill countered these claims, arguing that filtering is already common. Michael O'Leary of the MPAA testified on November 16 that the act's effect on business would be more minimal, noting that at

least 16 countries already block websites, and that the Internet still functions in those countries.[45] MPAA Chairman Chris Dodd noted that Google figured out how to block sites when China requested it.[46] Some ISPs in Denmark, Finland, Ireland and Italy blocked The Pirate Bay after courts ruled in favor of music and film industry litigation, and a coalition of film and record companies has threatened to sue British Telecom if it does not follow suit.[47] Maria Pallante of the US Copyright Office said that Congress has updated the Copyright Act before and should again, or "the U.S. copyright system will ultimately fail". Asked for clarification, she said that the US currently lacks jurisdiction over websites in other countries.[45]

Weakening of "safe harbor" protections

The 1998 Digital Millennium Copyright Act (DMCA) includes the Online Copyright Infringement Liability Limitation Act, that provides a "safe harbor" for websites that host content. Under that provision, copyright owners who felt that a site was hosting infringing content are required to request the site to remove the infringing material within a certain amount of time.[48][49][50] SOPA would bypass this "safe harbor" provision by placing the responsibility for detecting and policing infringement onto the site itself, and allowing judges to block access to websites "dedicated to theft of U.S. property".[51]

According to critics of the bill such as the Center for Democracy and Technology and the Electronic Frontier Foundation, the bill's wording is vague enough that a single complaint about a site could be enough to block it, with the burden of proof resting on the site. A provision in the bill states that any site would be blocked that "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 acts that constitute a violation". Critics have read this to mean that a site must actively monitor its content and identify violations to avoid blocking, rather than relying on others to notify it of such violations.[38][52]

Law professor Jason Mazzone wrote, "Damages are also not available to the site owner unless a claimant 'knowingly materially' misrepresented that the law covers the targeted site, a difficult legal test to meet. The owner of the site can issue a counter-notice to restore payment processing and advertising but services need not comply with the counter-notice."[53]

Goodlatte stated, "We're open to working with them on language to narrow [the bill's provisions], but I think it is unrealistic to think we're going to continue to rely on the DMCA notice-and-takedown provision. Anybody who is involved in providing services on the Internet would be expected to do some things. But we are very open to tweaking the language to ensure we don't impose extraordinary burdens on legitimate companies as long as they aren't the primary purveyors [of pirated content]."[54][55]

O'Leary submitted written testimony in favor of the bill that expressed guarded support of current DMCA provisions. "Where these sites are legitimate and make good faith efforts to respond to our requests, this model works with varying degrees of effectiveness", O'Leary wrote. "It does not, however, always work quickly, and it is not perfect, but it works."[23]

Web-related businesses

An analysis in the information technology magazine *eWeek* stated, "The language of SOPA is so broad, the rules so unconnected to the reality of Internet technology and the penalties so disconnected from the alleged crimes that this bill could effectively kill e-commerce or even normal Internet use. The bill also has grave implications for existing U.S., foreign and international laws and is sure to spend decades in court

challenges."[56]

Art Bordsky of advocacy group Public Knowledge similarly stated, "The definitions written in the bill are so broad that any US consumer who uses a website overseas immediately gives the US jurisdiction the power to potentially take action against it."[57]

On October 28, 2011, the EFF called the bill a "massive piece of job-killing Internet regulation", and said, "This bill cannot be fixed; it must be killed."[58]

Gary Shapiro, CEO of the Consumer Electronics Association, spoke out strongly against the bill, stating, "The bill attempts a radical restructuring of the laws governing the Internet", and that "It would undo the legal safe harbors that have allowed a world-leading Internet industry to flourish over the last decade. It would expose legitimate American businesses and innovators to broad and open-ended liability. The result will be more lawsuits, decreased venture capital investment, and fewer new jobs."[59]

Lukas Biewald, founder of CrowdFlower, stated, "It'll have a stifling effect on venture capital... No one would invest because of the legal liability."[60]

Booz & Company on November 16 published a Google-funded study finding that almost all of the 200 venture capitalists and angel investors interviewed would stop funding digital media intermediaries if the bill became law. More than 80 percent said they would rather invest in a risky, weak economy with the current laws than a strong economy with the proposed law in effect. If legal ambiguities were removed and good faith provisions in place, investing would increase by nearly 115 percent.[61]

As reported by David Carr of *The New York Times* in an article critical of SOPA and PIPA, Google, Facebook, Twitter and other companies sent a joint letter to Congress, stating "We support the bills' stated goals – providing additional enforcement tools to combat foreign 'rogue' Web sites that are dedicated to copyright infringement or counterfeiting. However, the bills as drafted would expose law-abiding U.S. Internet and technology companies to new uncertain liabilities, private rights of action and technology mandates that would require monitoring of Web sites."[31][62] Smith responded, saying, the article "unfairly criticizes the Stop Online Piracy Act", and, "does not point to any language in the bill to back up the claims. SOPA targets only foreign Web sites that are primarily dedicated to illegal and infringing activity. Domestic Web sites, like blogs, are not covered by this legislation." Smith also said that Carr incorrectly framed the debate as between the entertainment industry and high-tech companies, noting support by more than "120 groups and associations across diverse industries, including the United States Chamber of Commerce".[63]

Users uploading illegal content

Lateef Mtima, director of the Institute for Intellectual Property and Social Justice at Howard University School of Law, expressed concern that users who upload copyrighted content to sites could potentially be held criminally liable themselves, saying, "Perhaps the most dangerous aspect of the bill is that the conduct it would criminalize is so poorly defined. While on its face the bill seems to attempt to distinguish between commercial and non-commercial conduct, purportedly criminalizing the former and permitting the latter, in actuality the bill not only fails to accomplish this but, because of its lack of concrete definitions, it potentially criminalizes conduct that is currently permitted under the law."[64]

An aide to Rep. Smith said, "This bill does not make it a felony for a person to post a video on YouTube of their children singing to a copyrighted song. The bill specifically targets websites dedicated to illegal or

infringing activity. Sites that host user content—like YouTube, Facebook, and Twitter—have nothing to be concerned about under this legislation."[64]

Internal networks

A paper by the Center for Democracy and Technology claimed that the bill "targets an entire website even if only a small portion hosts or links to some infringing content".[49]

According to A. M. Reilly of *Industry Leaders Magazine*, under SOPA, culpability for distributing copyright material is extended to those who aid the initial poster of the material. For companies that use virtual private networks (VPN) to create a network that appears to be internal but is spread across various offices and employees' homes, any of these offsite locations that initiate sharing of copyright material could put the entire VPN and hosting company at risk of violation.[65]

Answering similar criticism in a CNET editorial, Recording Industry Association of America (RIAA) head Cary Sherman wrote, "Actually, it's quite the opposite. By focusing on specific sites rather than entire domains, action can be targeted against only the illegal subdomain or Internet protocol address rather than taking action against the entire domain."[66]

WTF? Does she know how the internet works?

Impact on web-browsing software

The Electronic Frontier Foundation expressed concern that free and open source software (FLOSS) projects found to be aiding online piracy could experience serious problems under SOPA.[67] Of special concern was the web browser Firefox,[33] which has an optional extension, MAFIAAFire Redirector, that redirects users to a new location for domains that were seized by the U.S. government.[68] In May 2011, Mozilla refused a request by the Department of Homeland Security to remove MAFIAAFire from its website, questioning whether the software had ever been declared illegal.[69][70]

Potential effectiveness

gets into gray area

Edward J. Black, president and CEO of the Computer & Communication Industry Association, wrote in the *Huffington Post* that "Ironically, it would do little to stop actual pirate websites, which could simply reappear hours later under a different name, if their numeric web addresses aren't public even sooner. Anyone who knows or has that web address would still be able to reach the offending website."[71]

just type in the #s

An editorial in the *San Jose Mercury-News* stated, "Imagine the resources required to parse through the millions of Google and Facebook offerings every day looking for pirates who, if found, can just toss up another site in no time."[72]

John Palfrey of the Berkman Center for Internet & Society commented, "DNS filtering is by necessity either overbroad or underbroad; it either blocks too much or too little. Content on the Internet changes its place and nature rapidly, and DNS filtering is ineffective when it comes to keeping up with it."[34]

Technical issues

then circumvent the knowledge that Pirate Bay is at 10.11.12.13

Deep-packet inspection and privacy

According to Markham Erickson, head of NetCoalition, which opposes SOPA, the section of the bill that would allow judges to order internet service providers to block access to infringing websites to customers located in the United States would also allow the checking of those customers' IP address, a method known as IP blocking. Erickson has expressed concerns that such an order might require those providers to engage in "deep packet inspection", which involves analyzing all of the content being transmitted to and from the user, raising new privacy concerns.[73][74] just encrypt!

Policy analysts for New America Foundation say this legislation would "instigate a data obfuscation arms race" whereby by increasingly invasive practices would be required to monitor users' web traffic resulting in a "counterproductive cat-and-mouse game of censorship and circumvention [that] would drive savvy scofflaws to darknets while increasing surveillance of less technically proficient Internet users".[39]

Domain Name System

The Domain Name System (DNS) servers, sometimes likened to a telephone directory, translate browser requests for domain names into the IP address assigned to that computer or network. The original bill requires these servers to stop referring requests for infringing domains to their assigned IP addresses. DNS is robust by design against failure and requires that a lack of response is met by inquiries to other DNS servers.[75]

Andrew Lee, CEO of ESET North America, objected that since the bill would require internet service providers to filter DNS queries for the sites, this would undermine the integrity of the Domain Name System.[76]

According to David Ulevitch, the San Francisco-based head of OpenDNS, the passage of SOPA could cause Americans to switch to DNS providers located in other countries who offer encrypted links, and may cause U.S. providers, such as OpenDNS itself, to move to other countries, such as the Cayman Islands.[77]

In November 2011, an anonymous top-level domain, .bit, was launched outside of ICANN control, as a response to the perceived threat from SOPA, although its effectiveness (as well as the effectiveness of other alternative DNS roots) remains unknown.[78]

On January 12, 2012, House sponsor Lamar Smith announced that provisions related to DNS redirection would be pulled from the bill.[79][80][81]

Internet security

A white paper by several internet security experts, including Steve Crocker and Dan Kaminsky, wrote, "From an operational standpoint, a resolution failure from a nameserver subject to a court order and from a hacked nameserver would be indistinguishable. Users running secure applications have a need to distinguish between policy-based failures and failures caused, for example, by the presence of an attack or a hostile network, or else downgrade attacks would likely be prolific."[82]

Domain Name System Security Extensions

Stewart Baker, former first Assistant Secretary for Policy at the Department of Homeland Security and former General Counsel of the National Security Agency, stated that SOPA would do "great damage to Internet security"[75] by undermining Domain Name System Security Extensions (DNSSEC), a proposed security upgrade for DNS, since a browser must treat all redirects the same, and must continue to search until it finds a DNS server (possibly overseas) providing untampered results.[75] On December 14, 2011 he wrote that SOPA was "badly in need of a knockout punch" due to its impact on security and DNS:[75]

> from the [Attorney General]'s point of view, the browser's efforts to find an authoritative DNS server will look like a deliberate effort to evade his blocking order. The latest version of SOPA will feed that view. It allows the AG to sue "any entity that knowingly and willfully provides ... a product ... designed by such entity or by another in concert with such entity for the circumvention or bypassing of" the AG's blocking orders. It's hard to escape the conclusion that this provision is aimed squarely at the browser companies. Browsers implementing DNSSEC will have to circumvent and bypass criminal blocking, and in the process, they will also circumvent and bypass SOPA orders.

DNSSEC is a set of protocols developed by the Internet Engineering Task Force (IETF) for ensuring internet security. A white paper by the Brookings Institution noted, "The DNS system is based on trust", adding that DNSSEC was developed to prevent malicious redirection of DNS traffic, and that "other forms of redirection will break the assurances from this security tool".[83]

On November 17, Sandia National Laboratories, a research agency of the U.S. Department of Energy, released a technical assessment of the DNS filtering provisions in the House and Senate bills, in response to Representative Zoe Lofgren's (D-CA) request. The assessment stated that the proposed DNS filtering would be unlikely to be effective, would negatively impact internet security, and would delay full implementation of DNSSEC.[84][85]

On November 18, House Cybersecurity Subcommittee chair Dan Lungren stated that he had "very serious concerns" about SOPA's impact on DNSSEC, adding, "we don't have enough information, and if this is a serious problem as was suggested by some of the technical experts that got in touch with me, we have to address it".[86]

Transparency in enforcement

Brooklyn Law School professor Jason Mazzone warned, "Much of what will happen under SOPA will occur out of the public eye and without the possibility of holding anyone accountable. For when copyright law is made and enforced privately, it is hard for the public to know the shape that the law takes and harder still to complain about its operation."[53]

Supporters

Legislators

Main article: List of US Congresspersons who support or oppose SOPA/PIPA

The Stop Online Piracy Act was introduced by Representative Lamar Smith (R-TX) and was initially co-sponsored by Howard Berman (D-CA), Marsha Blackburn (R-TN), Mary Bono Mack (R-CA), Steve

Chabot (R-OH), John Conyers (D-MI), Ted Deutch (D-FL), Elton Gallegly (R-CA), Bob Goodlatte (R-VA), Timothy Griffin (R-AR), Dennis A. Ross (R-FL), Adam Schiff (D-CA) and Lee Terry (R-NE). As of January 16, 2012, there were 31 sponsors.[87]

Companies and organizations

Main article: List of organizations with official stances on the Stop Online Piracy Act

The legislation has broad support from organizations that rely on copyright, including the Motion Picture Association of America, the Recording Industry Association of America, Entertainment Software Association, Macmillan US, Viacom, and various other companies and unions in the cable, movie, and music industries. Supporters also include trademark-dependent companies such as Nike, L'Oréal, and Acushnet Company.[88][89]

Both the AFL-CIO and the U.S. Chamber of Commerce support H.R. 3261, and many trade unions and industry groups large and small, have also publicly praised the legislation. In a joint statement, 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) all showed support for SOPA. Smaller trade organizations, such as A2IM, which represents independent musicians, have also backed the bill.[90]

In June 2011, former Bill Clinton press secretary Mike McCurry and former George W. Bush advisor Mark McKinnon, business partners in Public Strategies, Inc., started a campaign which echoed McCurry's earlier work in the network neutrality legislative fight. McCurry represented SOPA/PIPA in *Politico* as a way to combat theft on-line,[91] drawing a favorable comment from the MPAA.[92] On the 15th, McCurry and Arts + Labs co-chair McKinnon sponsored the "CREATE – A Forum on Creativity, Commerce, Copyright, Counterfeiting and Policy" conference with members of Congress, artists and information-business executives.[93]

On September 22, 2011, a letter signed by over 350 businesses and organizations—including NBCUniversal, Pfizer, Ford Motor Company, Revlon, NBA, and Macmillan US—was sent to Congress encouraging the passage of the legislation.[88][89] Fightonlinetheft.com, a website of The Coalition Against Counterfeiting and Piracy (a project of the United States Chamber of Commerce Global Intellectual Property Center,[94]) cites a long list of supporters including these and the Fraternal Order of Police, the National Governors Association, the U.S. Conference of Mayors, the National Association of Attorneys General, the Better Business Bureau, and the National Consumers League.[95][96]

On November 22 the CEO of the Business Software Alliance (BSA) said, "valid and important questions have been raised about the bill". He said that definitions and remedies needed to be tightened and narrowed, but "BSA stands ready to work with Chairman Smith and his colleagues on the Judiciary Committee to resolve these issues".[97][98]

On December 5, the Information Technology and Innovation Foundation, a non-partisan non-profit, published an article that blasted critics of SOPA and defended the bill. The report called opponents claims about DNS filtering "inaccurate", their warnings against censorship as "unfounded" and recommended that the legislation be revised and passed into law.[99]

On December 22, Go Daddy, the world's largest domain name registrar, stated that it supported SOPA.[100] Go Daddy then rescinded its support, its CEO saying, "Fighting online piracy is of the utmost importance, which is why Go Daddy has been working to help craft revisions to this legislation—but we can clearly do better. It's very important that all Internet stakeholders work together on this. Getting it right is worth the wait. Go Daddy will support it when and if the Internet community supports it."[101]

In January 2012, the Entertainment Software Association announced support for SOPA,[102] although some association members expressed opposition.[103] Creative America, a group representing television networks, movie studios, and entertainment unions, produced a "fact vs. fiction" flyer that aimed to correct misperceptions about rogue sites legislation.[104]

Others

Professor and Intellectual Property rights lawyer, Hillel I. Parness, a Partner of Robins, Kaplan, Miller & Ciresi[105] has reviewed the bill, stating in a legal analysis that "There's a court involved here." In regards to "safe harbors", he stated the safe harbor provisions created by the DMCA in 1998 would still apply. "I think the proponents of the bill would say, what we're looking at today is a very different kind of Internet. The fact that the courts have said that entities like YouTube can be passive when it comes to copyright infringement, and just wait for notices rather than having to take any affirmative action, is also frustrating to them", he said. Regarding censorship concerns, he explained that none of the criminal copyright statutes in the bill were new, and therefore, "if there was a risk of abuse, that risk has always been there. And I have confidence in the structure of our court system, that the prosecutors and the courts are held to certain standards that should not allow a statute such as this to be manipulated in that way."[106]

Constitutional law expert Floyd Abrams, on behalf of the American Federation of Television and Radio Artists (AFTRA), the Directors Guild of America (DGA), the International Alliance of Theatrical and Stage Employees (IATSE), the Screen Actors Guild (SAG), the Motion Picture Association of America (MPAA) and others,[107] reviewed the proposed legislation and concluded, "The notion that adopting legislation to combat the theft of intellectual property on the Internet threatens freedom of expression and would facilitate, as one member of the House of Representatives recently put it, 'the end of the Internet as we know it,' is thus insupportable. Copyright violations have never been protected by the First Amendment and have been routinely punished wherever they occur; including the Internet. This proposed legislation is not inconsistent with the First Amendment; it would protect creators of speech, as Congress has done since this Nation was founded, by combating its theft."[108] but the way it enforces things

White House position

On January 14, 2012, the Obama administration responded to a petition against the bill, stating that while it would not support legislation with provisions that could lead to Internet censorship, squelching of innovation, or reduced Internet security, it encouraged "all sides to work together to pass sound legislation this year that provides prosecutors and rights holders new legal tools to combat online piracy originating beyond U.S. borders while staying true to the principles outlined above in this response."[109][110][111][112] More than 100,000 people petitioned the White House in protest.[113] Three officials from the Obama administration articulated the White House's position on proposed anti-piracy legislation, balancing the need for strong antipiracy measures while respecting both freedom of expression and the way information and ideas are share on the Internet. "While we believe that online piracy by foreign websites is a serious problem

that requires a serious legislative response, we will not support legislation that reduces freedom of expression, increases cybersecurity risk, or undermines the dynamic, innovative global Internet."[114]

Opposition

Legislators

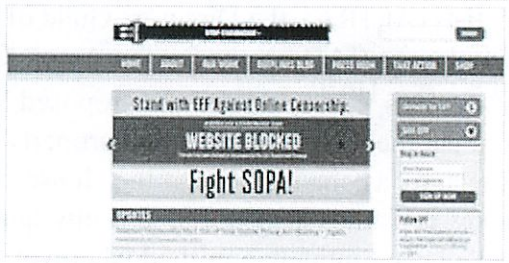
Main article: List of US Congresspersons who support or oppose SOPA/PIPA

House Minority Leader Nancy Pelosi (D-CA) expressed opposition to the bill, as well as Representatives Darrell Issa (R-CA) and presidential candidate Ron Paul (R-TX), who joined nine Democrats to sign a letter to other House members warning that the bill would cause "an explosion of innovation-killing lawsuits and litigation".[115] "Issa said the legislation is beyond repair and must be rewritten from scratch", reported *The Hill*.[116] Issa and Lofgren announced plans for legislation offering "a copyright enforcement process modeled after the U.S. International Trade Commission's (ITC) patent infringement investigations".[42] Politico referred to support as an "election liability" for legislators.[117] Subsequently proponents began hinting that key provisions might be deferred with opponents stating this was inadequate.[118][119] Representative Jared Polis (D-CO) has been known to lobby against SOPA in the game League of Legends, also making a post [120] in the official game message boards.[121]

Companies and organizations

Main article: List of organizations with official stances on the Stop Online Piracy Act

Opponents include Google, Yahoo!, YouTube, Facebook, Twitter, AOL, LinkedIn, eBay, Mozilla Corporation, Mojang, Roblox, Riot Games,[122][123] Epic Games (the developer of the game Gears of War), Reddit,[124] Wikipedia[125] and the Wikimedia Foundation,[126] in addition to human rights organizations such as Reporters Without Borders,[127] the Electronic Frontier Foundation (EFF), the ACLU, and Human Rights Watch.[128]



EFF home page with American Censorship Day banner

Kaspersky Lab, a major computer security company, demonstrated its opposition to SOPA and "decided to discontinue its membership in the BSA".[129]

On December 13, 2011, Julian Sanchez of the libertarian think tank Cato Institute came out in strong opposition to the bill saying that while the amended version "trims or softens a few of the most egregious provisions of the original proposal... the fundamental problem with SOPA has never been these details; it's the core idea. The core idea is still to create an Internet blacklist..."[130]

The Library Copyright Alliance (including the American Library Association) objected to the broadened definition of "willful infringement" and the introduction of felony penalties for noncommercial streaming infringement, stating that these changes could encourage criminal prosecution of libraries.[131]

On November 22, Mike Masnick of Techdirt called SOPA "toxic"[118] and published a detailed criticism[132]

of the ideas underlying the bill, writing that "one could argue that the entire Internet enables or facilitates infringement", and saying that a list of sites compiled by the entertainment industry included the personal site of one of their own artists, 50 Cent, and legitimate internet companies. The article questioned the effect of the bill on $2 trillion in GDP and 3.1 million jobs, with a host of consequential problems on investment, liability and innovation.[133] Paul Graham, the founder of venture capital company Y Combinator opposed the bill, and banned all SOPA-supporting companies from their "demo day" events. "If these companies are so clueless about technology that they think SOPA is a good idea", he asks, "how could they be good investors?"[134] Prominent pro-democracy movement, Avaaz.org started a petition in protest over SOPA and so far has got over 3.4 million signatures worldwide.[135]

The Center for Democracy and Technology maintains a list of SOPA and PIPA opponents consisting of the editorial boards of *The New York Times*,[31][136] the *Los Angeles Times*, 34 other organizations and hundreds of prominent individuals.[137]

Zynga Game Network, creator of Facebook games *Texas HoldEm Poker* and *FarmVille*, wrote to the sponsors of both bills highlighting concerns over the effect on "the DMCA's safe harbor provisions ... [which] ... have been a cornerstone of the U.S. Technology and industry's growth and success", and opposing the bill due to its impact on "innovation and dynamism".[138]

Others

Computer scientist Vint Cerf, one of the founders of the Internet, now Google vice president, wrote to Smith, saying "Requiring search engines to delete a domain name begins a worldwide arms race of unprecedented 'censorship' of the Web", in a letter published on CNet.[139][140]

On December 15, 2011, a second hearing was scheduled to amend and vote on SOPA. Many opponents remained firm even after Smith proposed a 71-page amendment to the bill to address concerns. NetCoalition, which works with Google, Twitter, eBay and Facebook, appreciated that Smith was listening, but says it nonetheless could not support the amendment. Issa stated that Smith's amendment, "retains the fundamental flaws of its predecessor by blocking Americans' ability to access websites, imposing costly regulation on Web companies and giving Attorney General Eric Holder's Department of Justice broad new powers to police the Internet".[141]

In December 2011, screenwriter and comics writer Steve Niles spoke out against SOPA, commenting, "I know folks are scared to speak out because a lot of us work for these companies, but we have to fight. Too much is at stake."[142][143]

In January 2012, novelist, screenwriter and comics writer Peter David directed his ire at the intellectual property pirates whose activities he felt provoked the creation of SOPA. While expressing opposition to SOPA because of his view that the then-current language of the bill would go too far in its restriction of free expression, and would likely be scaled down, David argued that content pirates, such as the websites that had posted his novels online in their entirety for free downloads, as well as users who supported or took advantage of these activities, could have prevented SOPA by respecting copyright laws.[144]

Twenty one artists signed an open letter to Congress urging them to exercise extreme caution, including Comedian Aziz Ansari, The Lonely Island music parody band, MGMT, OK Go, Jason Mraz and Trent Reznor of Nine Inch Nails. The letter reads, "As creative professionals, we experience copyright

infringement on a very personal level. Commercial piracy is deeply unfair and pervasive leaks of unreleased films and music regularly interfere with the integrity of our creations. We are grateful for the measures policymakers have enacted to protect our works. [...] We fear that the broad new enforcement powers provided under SOPA and PIPA could be easily abused against legitimate services like those upon which we depend. These bills would allow entire websites to be blocked without due process, causing collateral damage to the legitimate users of the same services - artists and creators like us who would be censored as a result."[145] Filmmaker Michael Moore also shut down his websites during the week of protest,[146] while other celebrities, including Ashton Kutcher, Alec Baldwin, and rapper B.o.B expressed their opposition via Twitter.[147][148] *The Daily Show*'s Jon Stewart stated that SOPA will "break the Internet".[149]

According to a NYT report (February 8, 2012), Art Brodsky of Public Knowledge said, "The movie business is fond of throwing out numbers about how many millions of dollars are at risk and how many thousands of jobs are lost ... We don't think it correlates to the state of the industry." The report also noted that "some in the internet world, including Tim O'Reilly, ... go so far as to question whether illegitimate downloading and sharing is such a bad thing. In fact, some say that it could even be a boon to artists and other creators." Tim O'Reilly is quoted as saying, "The losses due to piracy are far outweighed by the benefits of the free flow of information, which makes the world richer, and develops new markets for legitimate content ... Most of the people who are downloading unauthorized copies of O'Reilly books would never have paid us for them anyway."[150]

And offering a legit way to pay

International response

On November 18, 2011, the European Union Parliament adopted by a large majority a resolution that "stresses the need to protect the integrity of the global Internet and freedom of communication by refraining from unilateral measures to revoke IP addresses or domain names".[151][152]

Private individuals are petitioning the Foreign and Commonwealth Office, asking for the British government to condemn the bill.[153]

Vice-President of the European Commission and European Commissioner for Digital Agenda Neelie Kroes said she is "Glad [the] tide is turning on SOPA", explaining rather than having a "bad legislation" there "should be safeguarding benefits of open net". "Speeding is illegal too but you don't put speed bumps on the motorway", she said.[154]

Nonetheless, Ireland may have a law similar to SOPA passed soon - and "without Parliamentary vote". The Irish law is entitled, "S.I. No. 337/2011 — European Communities (Electronic Communications Networks and Services) (Universal Service and Users' Rights) Regulations 2011".[155][156]

Protest actions

Main article: Protests against SOPA and PIPA

On November 16, 2011, Tumblr, Mozilla, Techdirt, the Center for Democracy and Technology were among many Internet companies that protested by participating in American Censorship Day. They displayed black banners over their site logos with the words "STOP CENSORSHIP".[157]

Google linked an online petition to its site, and says it collected more than 7 million signatures from the

Mozilla's SOPA protest, displayed in Firefox on November 16, 2011.

United States.[158]

Markham Erickson, executive director of NetCoalition, told Fox News that "a number of companies have had discussions about [blacking out services]"[159] and discussion of the option spread to other media outlets.[160]

In January 2012, Reddit announced plans to black out its site for twelve hours on January 18, as company co-founder Alexis Ohanian announced he was going to testify to Congress. "He's of the firm position that SOPA could potentially 'obliterate' the entire tech industry", Paul Tassi wrote in *Forbes*. Tassi also opined that Google and Facebook would have to join the blackout to reach a sufficiently broad audience.[161] Other prominent sites that planned to participate in the January 18 blackout were Cheezburger Sites,[162] Mojang,[163] Major League Gaming,[164] Boing Boing,[165] BoardGameGeek, XKCD,[166] SMBC[167] and The Oatmeal.[168]

Wider protests were considered and in some cases committed to by major internet sites, with high profile bodies such as Google, Facebook, Twitter, Yahoo, Amazon, AOL, Reddit, Mozilla, LinkedIn, IAC, eBay, PayPal, Wordpress and Wikimedia being widely named as "considering" or committed to an "unprecedented" internet blackout on January 18, 2012.[169][170][171][172] On January 17 a Republican aide on Capitol Hill said that the protests were making their mark, with SOPA having already become "a dirty word beyond anything you can imagine".[173]

A series of pickets against the bill were held at the U.S. Embassy in Moscow. Two picketers were arrested.[174]

SOPA supporters complained that the bill was being misrepresented amidst the protests. RIAA spokesman Jonathan Lamy said, "It's a dangerous and troubling development when the platforms that serve as gateways to information intentionally skew the facts to incite their users and arm them with misinformation",[175] a sentiment echoed by RIAA CEO Cary Sherman who said "it's very difficult to counter the misinformation when the disseminators also own the platform".[176]

On January 21, 2012 RT news reported, "Bill Killed: SOPA death celebrated as Congress recalls anti-piracy acts". The Electronic Frontier Foundation, a rights advocacy non-profit group opposing the bill, said the protests were the biggest in Internet history, with over 115 thousand sites altering their webpages.[177]

Wikipedia blackout

The English Wikipedia blackout occurred for 24 hours on January 18–19, 2012. In place of articles, the site showed only a message in protest of SOPA and PIPA asking visitors to "*Imagine a world without free knowledge.*". It is estimated in excess of 160 million people

The English-language Wikipedia page on January 18, 2012, illustrating its international blackout in opposition to SOPA.

Sue Gardner at the Wikimedia Foundation on the evening of January 17, 2012, discussing the English Wikipedia blackout

saw the banner.[158] A month earlier, Wikipedia co-founder Jimmy Wales initiated discussion with editors regarding a potential knowledge blackout, a protest inspired by a successful campaign by the Italian-language Wikipedia to block the Italian DDL intercettazioni bill, terms of which could have infringed the encyclopedia's editorial independence. Editors and others[178] mulled interrupting service for one or more days as in the Italian protest, or alternatively presenting site visitors with a blanked page directing them to further information before permitting them to complete searches.[179][180] On January 16, the Wikimedia Foundation announced that the English-language Wikipedia would be blacked out for 24 hours on January 18.[181]

The *Daily Mail* estimated that 7,000 smaller websites either joined in the blackout for the day or posted some kind of protest at the proposed legislation.[182]

SOPA's sponsor in the House, Chairman Smith, called Wikipedia's blackout a "publicity stunt" saying: "It is ironic that a website dedicated to providing information is spreading misinformation about the Stop Online Piracy Act." Smith went on to insist that SOPA "will not harm Wikipedia, domestic blogs or social networking sites".[183]

Linked digital attack protest

Anonymous protesters in Guy Fawkes masks

On January 19, 2012, Megaupload, a website providing file sharing services, was shut down by the US Department of Justice and the Federal Bureau of Investigation.[184] This led to what Anonymous called "the single largest Internet attack in its history".[2] Barrett Brown, described as a spokesperson for the group Anonymous by the state-run[185] news outlet RT, said the timing of the raid "couldn't have come at a worse time in terms of the government's standpoint".[2] and said that the websites of the Justice Department, FBI, Universal Music Group, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and Broadcast Music, Inc had been shut down.[2] Some commentators and observers have asserted that the FBI shut down of Megaupload proves that SOPA and PIPA are unnecessary.[186][187] Although the actions of Anonymous received support, others have argued that the denial of service attack risked damaging the anti-SOPA case.[188][189][190]

The attack included a new, sophisticated method whereby internet users who clicked on links placed in chat rooms and on Twitter participated, some without their knowledge, in a denial of service attack, thereby breaking existing US law. Anonymous used "Low Orbit Ion Cannon" (LOIC) to attack supporters of SOPA on January 19, 2012. Anonymous claimed this to be their largest attack with over 5,635 people participating in the DDoS attack via LOIC.[191] LOIC was utilized by many attackers, despite the fact that a network firewall could easily filter out network traffic it generates, thus rendering it only partly effective. [*citation needed*] The group threatened to shut down Facebook's 60,000 servers in Operation Global Blackout on January 28, 2012.[192]

Legislative history

The House Judiciary Committee held hearings on November 16 and December 15, 2011. The Committee was scheduled to continue debate in January 2012,[193] but on January 17 Chairman Smith said that "Due to the Republican and Democratic retreats taking place over the next two weeks, markup of the Stop Online Piracy Act is expected to resume in February."[194] However, in the wake of online protests held on January 18, 2012, Rep. Lamar Smith has stated, "The House Judiciary Committee will postpone consideration of the legislation until there is wider agreement on a solution",[195] and Sen. Reid announced that the PIPA test vote scheduled for January 24 would also be postponed.[195][195][196][197]

November 16 House Judiciary Committee hearing

At the House Judiciary Committee hearing, there was concern among some observers that the set of speakers who testified lacked technical expertise. Technology news site CNET reported "One by one, each witness—including a lobbyist for the Motion Picture Association of America—said they weren't qualified to discuss... DNSSEC."[86] Adam Thierer, a senior research fellow at the Mercatus Center, similarly said, "The techno-ignorance of Congress was on full display. Member after member admitted that they really didn't have any idea what impact SOPA's regulatory provisions would have on the DNS, online security, or much of anything else."[198]

the basic split of the legislation

Lofgren stated, "We have no technical expertise on this panel today." She also criticized the tone of the hearing, saying, "It hasn't generally been the policy of this committee to dismiss the views of those we are going to regulate. Impugning the motives of the critics instead of the substance is a mistake."[199]

Lungren told Politico's *Morning Tech* that he had "very serious concerns" about SOPA's impact on DNSSEC, adding "we don't have enough information, and if this is a serious problem as was suggested by some of the technical experts that got in touch with me, we have to address it. I can't afford to let that go by without dealing with it."[200]

Gary Shapiro, CEO of the Consumer Electronics Association, stated, "The significant potential harms of this bill are reflected by the extraordinary coalition arrayed against it. Concerns about SOPA have been raised by Tea Partiers, progressives, computer scientists, human rights advocates, venture capitalists, law professors, independent musicians, and many more. Unfortunately, these voices were not heard at today's hearing."[59]

An editorial in *Fortune* wrote, "This is just another case of Congress doing the bidding of powerful lobbyists—in this case, Hollywood and the music industry, among others. It would be downright mundane if the legislation weren't so draconian and the rhetoric surrounding it weren't so transparently pandering."[201]

December 15 markup of the bill

Since its introduction, a number of opponents to the bill have expressed concerns. The bill was presented for markup by the House Judiciary Committee on December 15.

An aide to Smith stated that "He is open to changes but only legitimate changes. Some site[s] are totally capable of filtering illegal content, but they won't and are instead profiting from the traffic of illegal content."[202]

Markup outcome

After the first day of the hearing, more than 20 amendments had been rejected, including one by Darrell Issa which would have stripped provisions targeting search engines and Internet providers. *PC World* reported that the 22–12 vote on the amendment could foreshadow strong support for the bill by the committee.[203]

The Committee adjourned on the second day agreeing to continue debate early in 2012.[193][204] Smith announced a plan to remove the provision that requires Internet service providers to block access to certain foreign websites.[80] On January 15, 2012, Issa said he has received assurances from Rep. Eric Cantor that the bill would not come up for a vote until a consensus could be reached.[205]

See also

- Anti-Counterfeiting Trade Agreement (ACTA)
- Combating Online Infringement and Counterfeits Act (COICA)
- Commercial Felony Streaming Act
- Copyright bills in the 2011-2012 United States Congress
- Copyright Term Extension Act (CETA)
- Digital Economy Act 2010 (in the UK)
- Ley Sinde
- Protecting Children from Internet Pornographers Act of 2011
- Russian State Duma Bill 89417-6
- Cyber Intelligence Sharing and Protection Act
- Splinternet

References

1. ^ H.R.3261 – Stop Online Piracy Act (http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf) ; House Judiciary Committee; October 26, 2011
2. ^ *a b c d* "Internet strikes back: Anonymous' Operation Megaupload explained" (http://rt.com/usa/news/anonymous-barrettbrown-sopa-megaupload-241/) . *RT*. January 20, 2012. http://rt.com/usa/news/anonymous-barrettbrown-sopa-megaupload-241/. Retrieved January 21, 2012.
3. ^ Juliana Gruenwald (2011-12-08). "Critics of Online-Piracy Bills Release Their Own Draft Legislation" (http://www.nationaljournal.com/tech/critics-of-online-piracy-bills-release-their-own-draft-legislation-20111208) . NationalJournal. http://www.nationaljournal.com/tech/critics-of-online-piracy-bills-release-their-own-draft-legislation-20111208.
4. ^ "OPEN: Online Protection & Enforcement of Digital Trade Act" (http://keepthewebopen.com/) . keepthewebopen.com. http://keepthewebopen.com/. Retrieved 2012-01-11.
5. ^ House Introduces Internet Piracy Bill (http://www.washingtonpost.com/blogs/post-tech/post/house-introduces-internet-piracy-bill/2011/10/26/gIQA0f5xJM_blog.html) ; Washington Post; October 26, 2011
6. ^ H.R. 3261, STOP ONLINE PIRACY ACT (http://judiciary.house.gov/issues/issues_RogueWebsites.html) ; House Judiciary Committee; October 26, 2011
7. ^ Jim Abrams (19 January 2012). "PIPA and SOPA: What you need to know" (http://www.csmonitor.com/Innovation/2012/0119/PIPA-and-SOPA-What-you-need-to-know) . The Christian Science Monitor. http://www.csmonitor.com/Innovation/2012/0119/PIPA-and-SOPA-What-you-need-to-know.
8. ^ *a b* The US Stop Online Piracy Act: A Primer (http://www.pcworld.com/businesscenter/article/244011/the_us_stop_online_piracy_act_a_primer.html) ; PC World – Business Center; November 16, 2011
9. ^ *a b c* "Bill Summary by Congressional Research Service" (http://www.webcitation.org/643NehNoc) . Thomas – Library of Congress. October 26, 2011. Archived from the original (http://thomas.loc.gov/cgi-bin

Online Protection and Enforcement of Digital Trade Act

From Wikipedia, the free encyclopedia

The **Online Protection and Enforcement of Digital Trade Act** (**OPEN Act**) is a bill introduced in the United States Congress proposed as an alternative to the Stop Online Piracy Act and PROTECT IP Act, by Senator Ron Wyden of Oregon, a Democrat, and Representative Darrell Issa of California, a Republican.[1][2][3][4][5] The text of the bill is available for public comment at keepthewebopen.com (http://keepthewebopen.com/) .[6]

Wyden first introduced OPEN in the Senate (**S. 2029**) on December 17, 2011 with co-sponsors Jerry Moran of Kansas and Maria Cantwell of Washington. Issa and 25 co-sponsors introduced OPEN in the House (**H.R. 3782**) on January 18, 2012. The Senate bill has been referred to the Finance Committee, and the House bill has been referred to the Judiciary Committee.[7][8][9]

On January 14, 2012, in response to two White House petitions, White House technology officials Victoria Espinel, Aneesh Chopra, and Howard Schmidt stated: "Any effort to combat online piracy must guard against the risk of online censorship of lawful activity and must not inhibit innovation by our dynamic businesses large and small...We must avoid creating new cybersecurity risks or disrupting the underlying architecture of the Internet."[10][11][12][13]

Contents

- 1 Comparison with SOPA and PIPA/PROTECT IP Act
- 2 Reception
- 3 Public comment using Madison
- 4 Supporters
  - 4.1 Senate
  - 4.2 House
- 5 References
- 6 External links

Comparison with SOPA and PIPA/PROTECT IP Act

The OPEN Act was proposed as an alternative to the PROTECT IP Act (PIPA), which was approved by the United States Senate Judiciary Committee in May 2011, and the closely related Stop Online Piracy Act (SOPA), which was introduced by House Judiciary Chairman Lamar Smith (R-TX) in November. After an initial description on December 2 as an outline of possible approaches written by a bipartisan group of eleven lawmakers,[14][15] a draft text was made public on December 8, 2011 in advance of a House Judiciary markup of the SOPA Act the following week. The OPEN Act seeks to stop transfers of money to foreign websites whose primary purpose is piracy or counterfeiting, whereas SOPA and PIPA also seek to require Internet providers and search engines to redirect users away from viewing the sites. The PROTECT

IP Act proposed to do this by blocking domain name resolution, whereas SOPA imposes a broader requirement for network providers to "prevent access by its subscribers located within the United States" including blocking by IP address and possibly deep packet inspection.[3]

OPEN places enforcement responsibility on the United States International Trade Commission (ITC), which currently adjudicates patent-related disputes, rather than the United States Justice Department.[5] The ITC would be given power to collect fees from complainants and to hire additional personnel for investigations.[2]

Proponents of the OPEN Act describe it on the KeepTheWebOpen website as a way to protect the rights of artists like SOPA and PROTECT IP, but differing from its rivals by not introducing new internet police powers or undermining calls for open internet in closed societies, and by protecting legitimate internet businesses, social media, legitimate websites and internet innovation. They say that their proposal, but not its rivals, ensures that intellectual property cases will be resolved by intellectual property experts, and will target the actual criminals running foreign rogue websites. They criticize SOPA, but not PROTECT IP, for failing to apply due process to judging websites.[16]

Reception

The OPEN draft is backed by Web companies such as Google and Facebook, whereas SOPA and PIPA are backed by the movie and music industries.[2][17]

The Consumer Electronics Association commended the sponsors of the bill, calling it "a quick, effective way to shut down pirate sites without damaging legitimate companies or enriching trial lawyers."[18] The bill was also praised by the Computer and Communications Industry Association.[19] Google copyright counsel Fred von Lohmann said for his company, "We think following the money, the money that supports foreign rogue sites, is a sensible place to start. It was quite successful in offshore gambling... We've been very clear with members of the committee that we support that."[3]

The OPEN draft was strongly opposed by the Motion Picture Association of America (MPAA). The MPAA's vice president of global policy and external affairs, Michael O'Leary, wrote in the MPAA's blog that the bill "allows companies profiting from online piracy to advocate for foreign rogue websites against rightful American copyright holders. It even allows notification to some of these companies if they want to help advocate for rogue websites."[20][21] The MPAA rejects any law that fails to block Americans' access to The Pirate Bay, a BitTorrent tracker which survived prosecution in its home country of Sweden and steadfastly refuses to remove information about infringing downloads from its search index. Darrell Issa maintains that the OPEN act could be effective against the site by targeting even overseas ad networks placing ads on the site, though it is possible that the site could survive without advertisements.[22][23]

The Electronic Frontier Foundation (EFF) wrote that the legislation "addresses many of the most glaring flaws in both SOPA and PIPA" but stated that it is continuing to review and analyze the draft.[1] Public Knowledge deemed the bill a "marked improvement" that would avoid the "vigilante justice" of its rivals.[19] Center for Democracy and Technology senior policy counsel Eric Sohn said that the bill's definitions "appear to carefully target true bad actors--the ones who are willfully fostering widespread infringement--while excluding general purpose platforms and social networking services," whose financial focus would "starve those bad actors of their financial lifeblood, rather than pursuing the futile and costly approach of messing

with the Internet's addressing system."[3]

Copyright Alliance executive director Sandra Aistars called the OPEN Act "impractical for individual artists and creators", who would be required to argue in Washington before the trade commission rather than in their home jurisdictions, during a period of up to 18 months.[24] The process would be much faster, however, for sites that fail to reply and participate in the ITC process, according to Issa, who note that the ITC has a "rocket docket" in which cases are heard more quickly than any federal court.[25] Writing in the Huffington Post, Aistars argued that the bill placed more obstacles for individual artists than for corporate litigants seeking patent remedies before the ITC, saying that fees proposed for complainants in the action were "unprecedented" and incompatible with "justice for all", while third parties profiting from the infringement could argue for the decision to be overturned by the Administration without paying any fee. She further stated that the hearing officers assigned to hear cases by the bill were not required to have intellectual property expertise, and that the evidentiary requirement for a site owner to "willfully" commit infringement would be a mental state impossible to prove for rogue operators refusing to consent to U.S. jurisdiction.[26]

Professor Eric Goldman of the Santa Clara University School of Law reviewed the bill in detail for Ars Technica, finding it "flawed, but more salvageable" than "SOPA's disgustingly blatant rent-seeking" and praising the bill's due process features and a focus on foreign trade policy. However, Goldman also warned that the burden on U.S.-based payment service providers and ad networks could drive business to foreign competitors and permit domestic and foreign legal action simultaneous with the ITC administrative proceeding, or other abuses.[27]

Forbes ran a column denouncing the bill as "politically untenable" and "not a viable alternative because it is a transparent attempt to return a several year effort back to square one, while also entangling it with thorny and debilitating congressional jurisdictional turf battles and even thornier and glacial trade policy politics."[28]

Nonetheless, in support of OPEN, *The New York Times*, in an editorial, notes "...[OPEN] gives copyright holders powerful new tools to protect themselves. And it goes a long way toward addressing the concerns of Internet companies, protecting legitimate expression on the Web from overzealous content owners."[29]

Public comment using Madison

The call for public comment on the draft was described by CNet News as "the Wiki-fication of part of the legislative process." Site visitors can read the text of the bill and suggest specific edits[3] on Madison, described as a "digital legislative platform that lets anyone suggest changes to the draft bill, a Wikipedia of sorts for legislative text."[30]

Supporters

The following members of Congress support the Online Protection and Enforcement of Digital Trade Act.[31]

Senate

- Maria Cantwell (D-WA)

Chat 10/11

Julian Gonzalez: *00:12* can we chat here?
ssuen: *00:12* sounds good
ssuen: *00:12* anyone get in touch with MG?
Jacob Bennett: *00:13* nope
ssuen: *00:13* ok nvm
Julian Gonzalez: *00:15* okay, so i'm on the content distribution side
Julian Gonzalez: *00:15* jacob, you with me?
Jacob Bennett: *00:15* yep
ssuen: *00:15* so is that still tied in with sopa/pipa
Jacob Bennett: *00:15* But let's try to find something first.
ssuen: *00:15* or is this a new idea
Jacob Bennett: *00:15* It will still be tied in with SOPA/PIPA at this point.
ssuen: *00:16* k
Julian Gonzalez: *00:17* okay, so the other idea is CISPA?
Julian Gonzalez: *00:17* is that enough meat for a paper?
Jacob Bennett: *00:18* Well, both topics need a greater focus on a policy change at this point. imo
ssuen: *00:19* victoria, thoughts?
Julian Gonzalez: *00:19* so for the idea we were thinking about, jacob, are we focusing on promoting the development of good content distribution systems, like steam
Julian Gonzalez: *00:20* itunes, hulu?
Jacob Bennett: *00:20* Also, if we divide, will Michael Plasmier join one of the two groups?
ssuen: *00:21* wait are you talking about MG or someone else
Jacob Bennett: *00:21*Somebody else, don't know if you saw this email thread, but someone from another group wants to move to our group.
ssuen: *00:22* oh ok
ssuen: *00:22* that's good then
ssuen: *00:22* i was worried about the 2-person group for a sec
Jacob Bennett: *00:24* Yeah, me too. Thought I would mention it.
Jacob Bennett: *00:24* Be back in 5 min.
Julian Gonzalez: *00:25* so steven, do you have any thoughts either way?
ssuen: *00:25* ok
ssuen: *00:25* just trying to think how to translate the business-oriented analysis of successful distribution platforms
ssuen: *00:26* to actual legal/policy advice
Julian Gonzalez: *00:32* hmm
Jacob Bennett: *00:39* k im back
victoria sun: *00:42* wow i failed to notice this chat window
ssuen: *00:43* lol
ssuen: *00:44* so, to recap
ssuen: *00:44* we're splitting into two groups of 3
ssuen: *00:44* which means two proposals
Jacob Bennett: *00:45* that should happen, let me contact Michael before anything happens.
ssuen: *00:45* k
ssuen: *00:45* i mena
ssuen: *00:45* i mean*
ssuen: *00:45* at this point
ssuen: *00:45* we just want to finalize our two ideas
Julian Gonzalez: *00:45* yep
Julian Gonzalez: *00:45* then we can write the proposal
ssuen: *00:45* yup
victoria sun: *00:48* wait
victoria sun: *00:48* who is in what group now then
ssuen: *00:48* we're going to decide the two topics first
ssuen: *00:48* and then divide from there
victoria sun: *00:48* i see
victoria sun: *00:48* hrm im pretty sure danny is okay with a large group
victoria sun: *00:48* i think that 5 is okay, personally
ssuen: *00:49* apparently hal said no
ssuen: *00:49* and another person wanted to switch into the group
victoria sun: *00:49* yeah but there are a lot of gorups with a lot of people
theplaz: *00:49* so I talked with Hal and he said he is uncomfortable with 5
theplaz: *00:49* "I think that even 5 is too much."
victoria sun: *00:49* im aware of that

victoria sun:00:49 i saw the email
theplaz:00:49 ok
victoria sun:00:49 but since groups aren't finalized until this week anwyays
victoria sun:00:50 i think that we're better off doing one proposal and discussing this more later
victoria sun:00:50 since there are many groups that are greater than 3 in the clas
victoria sun:00:51 also in speaking to danny he okayed our group of 5
victoria sun:00:51 which is why i emailed you (michael) saying that you should try contacting the other copyright gorup first
Jacob Bennett:00:52 I brought plaz into the discussion since I was unaware that 5 people in a group is acceptable.
victoria sun:00:53 sorry -- i didn't fill the rest of you guys in on what was happening since it didn't seem super relevant unless michalel was definitely
victoria sun:00:53transferring into our group
victoria sun:00:54 but if you recall danny was okay with our copyright superteam initially of like 10 people
victoria sun:00:54 and suggested we make a 5 and a 4
ssuen:00:55 yeah
victoria sun:00:58 i'm uncomfortable with how long this conversation has gone on and i think that our original plan of us 5 writing this proposal and then
victoria sun:00:58 revisiting how we want to split
victoria sun:00:58 is best
theplaz:00:58 let's see how our interests actually line up
victoria sun:00:59 look, htis paper is already late
victoria sun:00:59 we can match interests on thursday
ssuen:00:59 ok
ssuen:00:59 gonna copy the super generic stuff i wrote earlier here
theplaz:00:59 or if we write a propsal with 6 then talk in class if/how split
theplaz:01:00 with danny and hal
ssuen:01:00 yeah
theplaz:01:00 so we don't get 2 sep answers
ssuen:01:00 that sounds reasonable
victoria sun:01:00 i'm not comfortable iwth that
ssuen:01:00 wait what
ssuen:01:00 isn't that what you were suggesting
ssuen:01:00 write one proposal now
ssuen:01:00 and split later
victoria sun:01:00 no i was suggesting we go with the original 5 on the proposal like danny approved of
ssuen:01:00 oh
ssuen:01:01 cuz the other group has 4 huh
victoria sun:01:01 yeah
victoria sun:01:01 i'd just rather stick with a concrete answer we're all aware of
victoria sun:01:01 which is that danny approved of all the groups as they were last thursday
victoria sun:01:04 michael are you comfortable with contributing to this paper knowing htat you might not be creditted for it?
theplaz:01:08 victoria - i don't know what all the drama is about
theplaz:01:08 we got 2 different answers from 2 different professors
theplaz:01:09 let's go with something and resolve it in class
victoria sun:01:09 i prefer to go with the answer that makes the most sense to me which is to stick with the status quo
victoria sun:01:09 it's a relatively low drama answer
theplaz:01:09 i perfer to go by latest answer from a course staff member, which was CCed to 6.805-staff
theplaz:01:10 I mean this is a silly debate to be having
theplaz:01:10 let's actually see where our interests lie
theplaz:01:10 and some of us might be interested in diff directions
theplaz:01:10 that is what the above text seems like
victoria sun:01:10 which is what we were supposed to establish last week in clas
victoria sun:01:11 there's a last original group member whose opinion is lacking
ssuen:01:12 MG's not around
theplaz:01:12 so right now Ssuen and jacob bennett seem interested in a market analysis on OTT
victoria sun:01:12 yeah :\ he has the most knowledge on this topic too i feel lkike
ssuen:01:13 not really
theplaz:01:13 ok, sorry
ssuen:01:13 i'd like to do more analysis of SOPA
ssuen:01:13 haha
theplaz:01:13 im just looking at your colors

victoria sun: *01:13* i'm pretty sure that we're all in the SOPA analysis camp
ssuen: *01:13* oh that was just copypasta'd from the original doc
theplaz: *01:13* oh ok - sorry
ssuen: *01:13* anyway for now let's just do one proposal because i don't think we have the manpower nor the time to churn out two
victoria sun: *01:13* where is mg?
ssuen: *01:14* please read over what i've got so far and make any changes as you see fit
Julian Gonzalez: *01:17* SOPA also had a fraud aspect to it...to prevent things like selling prescription drugs from shady doctors
Julian Gonzalez: *01:18* it's not too significant though
victoria sun: *01:19* we probalby don't need to address it too much in detail
victoria sun: *01:19* its just a proposal outlining what we're going to do
ssuen: *01:19* 1 page though?
victoria sun: *01:19* not all the details of it
ssuen: *01:19* haha
ssuen: *01:20* ok
theplaz: *01:20* right
victoria sun: *01:20* stephen -- what esle do you need to write this? i think there's a decent amount of ocntent in here
ssuen: *01:20* k
victoria sun: *01:20* i htink you can also include the open questions we have too
ssuen: *01:20* sure
victoria sun: *01:20* like "we will develop metrics to define success" etc
theplaz: *01:23* should we include a section on our backgrounds for our mentor(s)?
victoria sun: *01:24* no
theplaz: *01:25* ok
theplaz: *01:40* so are these open questions that we are trying to answer
theplaz: *01:41* or questions that will remain open after our paper
victoria sun: *01:41* that we anticipate answering
ssuen: *01:42* lol yeah
Julian Gonzalez: *01:43* yup
ssuen: *01:43* i'm kind of making shit up right now
ssuen: *01:43* so if you have any good ideas
ssuen: *01:43* add em
theplaz: *01:44* i agree; let's put everything in now
theplaz: *01:44* and then the professors/mentors can tell us where to focus
ssuen: *01:44* yep
ssuen: *01:44* sounds good
theplaz: *01:48* so if you copy that into Word its about 1 pg
ssuen: *01:48* yah
ssuen: *01:48* cool
ssuen: *01:48* i think this looks okay
ssuen: *01:48* let's get our names on it and turn it in?
ssuen: *01:48* do you have everyone's name
victoria sun: *01:49* stephen can you turn it in?
Julian Gonzalez: *01:49* looks good
ssuen: *01:49* ok
ssuen: *01:49* i'll turn it in
ssuen: *01:50* gimme a sec
victoria sun: *01:50* do you need a list o fnames?
ssuen: *01:50* i think i got them
victoria sun: *01:50* kk

10/1

NOTE: On the top right, there's a "user" icon. Click it and change your name. That way we can see who's typing what. It'll automatically color-code your text.

summary of our paper ideas as discussed in class:
- survey of SOPA, PIPA, CISPA?, etc // recent legislation related to internet piracy and copyright infringement/enforcement
- analysis of their effects should they be instantiated
- recommendations of how they should be improved, including promoting business models such as hulu where constructing new delivery sources is encouraged

hulu/youtube/steam/itunes/netflix:
http://en.wikipedia.org/wiki/Over-the-top_content -- over-the-top content = broadband delivery of video and audio without internet service provider being involved in the control or distribution of content itself subscription service

hulu:
revenue: $420 million in 2011
aprox 1.5 million hulu plus subscribers

suggestion by Jacob Bennett (more to come):
-I say we narrow our SOPA pov to sometthing directly relating to Over-the-top content/content distribution systems. what about them?well, that's the million dollar question. I haven't figured out yet, still researching. k
like do we want to propose a business model that might work
I think the Studios have done the #s and where as they will make some money on over the top (more than piracy) they will canbolize legit sales
So lets say (making up #s) they make 100M from current legit channels and lose 20M (assume accurate estimate)
If they establish a legit site they could make 30M but then 40M of legit business will switch to OTT
Or it's because of a long standing structure of contracts that take time to unwind
I talked with a SVP at Disney/ABC Online this summer about this very issue
-Again, we must focus on a specific policy goal. Let me gather some more research.
-Perhaps tie something in directly with CDNs [Content Delivery Networks]
-If we want perform a schism, would it be (CISPA) v. (SOPA and content distrobution)?

suggestions from Julián G:
- investigation of problem of internet piracy in general; put problem in context
- look at successful content distribution systems: Steam, iTunes, Hulu (what do we call "successful" anyway?) and identify several concepts that they do "right", and "wrong"
- then, when recommending improvements to current US law or recommending an approach to directing the law take those ideas in mind
- show how chilling effects of acts like SOPA and PIPA would be lessened or eliminated under our recommendations
- again, look at OPEN, which does not solve the problem, but has interesting suggestions

Michael Plasmeier theplaz:
I'm interested in how we can rewrite SOPA to attack piracy without harming the internet
That would likly involve a long review of SOPA/PIPA to review what was harmful and why
And reviewing the policy mechansims that might actually address piracy
ie. defunding advertising networks

not. DNS changes - able to be twarted, would hurt DNSSEC, effectivly preventing distribution of IP addresses might be free speech violation - IDK - say if you were not allowed to speak the address of a house known to sell drugs

~~We will review the historic DMCA and its impact on the piracy of copyrighted materials over the last four years it has been in force. We will review key provisions and their effects on both preventing illegal services and <I think we can skip to open questions/areas of further exploration. If you want to mention DMCA add it to paragraph 1 when I talk about history ok. i just had it in a temp buffer cool np>~~
~~>>~~

~~<I also want to include somewhere how UGC sites like YouTube have been possible due to the DMCA - and how vol. agreements have shaped the industry>~~

feel free to make changes / add stuff below:

← Submitted proposal

Semester Project Proposal: Post-Mortem of Online Piracy Bills

2012 was a landmark year for copyright legislation: SOPA and PIPA—and the resulting mobilization of the Internet community against these bills—brought issues of intellectual property enforcement back into the popular consciousness. Why did public opinion on these bills, which initially enjoyed broad bipartisan support, turn so dramatically in such a short period of time? In our semester project, we will retrospectively analyze the legal and technical factors that contributed to the failure of these online piracy bills. First, we will attempt to put the problem of Internet piracy into context, giving a broad overview of the development of modern copyright legislation, as well as a portrait of the market and legal environment that gave rise to SOPA/PIPA. We will review the tools currently available to rights holders and law enforcement, including the DMCA. Then, we will dissect the contents of the SOPA and PIPA bills from different perspectives, and analyze the potentially harmful effects they might have had on the Internet had they been passed, including implications for free speech, intermediary liability, cybersecurity, privacy, and web-based innovation at large. Based on these issues, the goal of this report will be to identify possible policy actions to address the piracy problem without harming the underlying structures of the open Internet and the civil liberties guaranteed by those structures.

To this end, we'll analyze the problem from both a business-oriented and a more policy-focused perspective. In the former, our report will cross-sectionally examine successful digital distribution platforms and how they have (and have not) managed to circumvent the issue of online piracy. We will review how user-generated-content sites such as YouTube, have navigated the market, looking at both statutory requirements and voluntary agreements between the technology platforms and content owners. We will also look at currated distribuitors. This will include case studies from the worlds of video gaming (e.g. Steam, Humble Indie Bundle), music (e.g. iTunes, Spotify), and television/film (e.g. Hulu, Netflix). We will attempt to answer the question why more content providers have not made larger investments in over-the-top television services. Identifying the key successes and failures of these services, we will attempt to translate these insights into concrete policy advic e. In the latter, we will investigate proposed policy mechanisms designed to address piracy (e.g. defunding advertisement networks, DNS changes), and assess their viability and effectiveness. We will also examine the suggestions laid out in OPEN, the bill proposed as an alternative to SOPA. To put this analysis into perspective, we will review the existing studies on the losses of the industry from pirated material. Moreover, we will attempt to categorize the losses due to piracy into a number of categories, so that we are better able to analyze which policy mechanism would be most effective at preventing piracy. This will require designing some sort of metric for evaluating the piracy-fighting effectiveness of each of these proposed solutions.

As we delve into our research and continue to develop this topic, there are a number of open questions worth exploring further. For one, we will do a comparative analysis of copyright law pre- and post-Internet, to see how notions of intellectual property and proper enforcement of those exclusive rights have changed over time. It would be interesting to see the evolution of the public discourse around SOPA and PIPA over time, particularly looking at the effects of the Internet blackout observed by Wikipedia and other websites. It might also be worthwhile to look at the lasting effect the debate over these bills has had on the Internet community's involvement in politics, looking at the more recent efforts to establish an Internet Defense League as well as the push to get Internet users registered to vote. It will also be worth investigating similar legislative efforts overseas; for example, international treaties such as ACTA. How are the supporters of SOPA and PIPA planning to move forward after public opinion turned againts them. What will be their next move?

Users:
Stephen J Suen <ssuen@mit.edu>
Julian A Gonzalez <jugonz97@mit.edu>
Jacob A Bennett <bennettj@mit.edu>
Victoria Sun <vsun@MIT.EDU>
Michael E Plasmeier <theplaz@MIT.EDU>
Michael V Grinich <grinich@mit.edu>

Michael E Plasmeier

From: halatmitdotedu@gmail.com on behalf of Hal Abelson <hal@MIT.EDU>
Sent: Wednesday, October 03, 2012 9:42 AM
To: Stephen J Suen; Victoria S Sun; Michael Grinich; Julian A Gonzalez; Michael E Plasmeier; Jacob A Bennett
Cc: 6.805-staff
Subject: comments on team report

Follow Up Flag: Follow up
Flag Status: Completed

Nice job putting this together! It raises lots of interesting issues, and it's very well written.

But there are two big concerns from the perspective of a term project.

First, your group is too large. Please split it into two groups of three. The goal is that everyone on the the team will have a clear, major role to play in shaping the entire report; and that's not practical with a team of more than four.

Second, and related, the area you've scoped out is too vast. You need to focus on a particular issue that the new Admonostration will need to address, and where you can do something in depth that makes a contribution – not just review a broad area where there are hundreds (thousands?) of papers already written.

I'd stay away from the international issues: there's a whole other group already working on that.

Another thing to remember is that the reason people might care about what you would write is that *you are MIT students*. So how can you draw on your technical skills to produce new insights or points of view?

So split into two topics. A recommendation to the administration on whether to support OPEN (of suggested variations) in post-SOPA world might be a good topic – provided you back it up with the kind of analysis you hint at.

Another topic might grow out of the comments you make about high-tech lobbying and the internet defense league, but if you go in that direction, you should get advice from Alan about what a productive policy question might be.

Another topic might be to look at the DMCA notice and takedown mechanism and see how that holds up in the age of content id and the technilogies that will follow on from that.

Please be ready on Thursday to discuss how you'll split the group, and what (two) policy issues you will explore.

==Hal
hal@mit.edu

Michael E Plasmeier

From: s2tephen@gmail.com on behalf of Stephen J Suen <ssuen@MIT.EDU>
Sent: Thursday, October 04, 2012 10:14 PM
To: Michael E Plasmeier
Subject: 6.805 Paper

Follow Up Flag: Follow up
Flag Status: Flagged

Hey Michael:

Quick update about the 6.805 final paper—after some discussion, our group is splitting up into two smaller groups. The other four members all wanted to work on the CDN/open licensing business analysis, so the two of us will have to work together. Thing is, another group has already claimed the topic of analyzing OPEN; we can still do something SOPA-related but it's going to have to be a more specific/narrow topic than what you had indicated in your previous email of interest. We need to turn in an updated proposal by Sunday so that we can get assigned a mentor in a timely fashion.

I voiced some concern to Danny about working in a group of two, but he reassured me that it will still be doable and we will have less logistical overhead with fewer members. If you'd rather work in a larger group (i.e. return to your old group), I understand, but please let me know ASAP so that I can find another group to transplant myself onto. If you're willing to work with me, that's cool too, but we'll need to brainstorm a new topic. Here are some ideas that I've been floating around:

- Analyzing the creative/economic value of alternative licensing schemes like Creative Commons, evaluating criticisms and legal challenges, and giving policy suggestions as to how to better promote such licenses
- Looking at the evolution of YouTube's copyright policies, particularly DMCA takedowns/appeals and the Content ID system in relation to user practices (http://youtubecreator.blogspot.com/2012/10/improving-content-id.html)
- Examining the effectiveness of DRM across different media (video games, music, movies, books), assessing the legal issues presented, and proposing possible alternatives
- Comparing the dynamics of online legal remix communities like hitRECord, Scratch to those in legal gray area, e.g. AO3/fanfics, Soundcloud/remixes, Deviantart/fanart, YouTube/fanvids, etc

Let me know if any of these appeal to you or feel free to suggest some of your own. I'm going to be in Vermont this weekend with limited internet access so I'd like to get this done ASAP.

Thanks!

--
Stephen J Suen / ssuen@mit.edu / @s2tephen
Massachusetts Institute of Technology
Class of 2015 – Comparative Media Studies

Steven Sieg

6.805 Mtg

10/5

4 people

electronic sell through + online streaming biz models

how gov could intervene to promote

Open group → doing sorting

---

be narrower

leverage analysis of MIT students

SOPA over analyzed

cracking down on piracy

review of methods to address piracy

are effective

SOPA

Open) but not

then policy suggestions

0

Demi Policy advice in whole thing → not thrown in end

TA: Andrew

Concrete list

- brainstorm

best are two

New LeBOS
Proposal

10/7
YP

* A review of policy methods to address piracy

Vish Steven was ~~here~~ editing w/ me
His poposal was better...

; do we mention SOPA + PIPA in opening para
kinda related
but not a focus of the article

Write list para list then rearrange

---

need to get a more comprehensive list

Project Meeting

10/19

NN project

I am applying conflict research prompt to this project
- Understand contravery for us internally
- Write it up + share

but prof must not just a policy brief
- Something new

(hone in on something
- Lit review
- Guiding principles
- Criteria - measurable;
- tool - 6 stiles
- Policy rec

(very good brainstorming - I'm aware of doing it now)

list of metrics + guildlines
- not economic

(2)

General + broad

- iTunes sales ?
- how measure how much piracy there is ?
- $ lost revenue

- do more research
- things to look at

- Movies, Music, TV - all 3 + compare
- lost sales
- BitTorrent traffic
- Netflix + Redbox streams/rentals
- Say we to ask our mentors
- Pick an angle

(3)

least political resistance

least politically objectionable

least impact on internet - MIT perspective

Steven has OK/ basic knowledge of how DNS works

Willing to read

CMS/Core 6

HCI stuff

Mention economic, but not

Objectives

metrics

Principal: Don't break internet

Motive - Still allow robust DNS SEC implementations

Paradigm shifts

Old agreements looked good

but are now actually bad

4

To review

Revenue

↑ sales

employment

record company vs artists

- less important
- ideological debate

↓ PBL

Reduces piracy

not circumvented

Implementation

Who

Costs

Politics/stakeholders

Industry

Citizens

Artists

(5)

Negative ~~reproduction~~ repercussions on interest
Creativity of interest

Will it disrupt biz models

Mei: Don't get too much into the weeds

Unintended Consequences
Non infringing use] ⇒ Meag update take down

Chain
effective ⇒ circumvention ⇒ revenue ⇒ jobs

Submitted 10/20

6.805 Semester Project Scope — Michael E Plasmeier, Stephen J Suen

In order to better focus the direction of our final project, we have devised a basic skeleton for the paper and the framework contained within. Hopefully this should give you a better idea of our intended project scope, what specific issues we want to focus on, and in what capacities a mentor might be able to assist us. The structure of the paper will flow as follows:

1. Review of current literature on evaluating the economic costs of piracy and on assessing the effectiveness of anti-piracy mechanisms
2. The details of the evaluative framework itself
    a. Abstract guiding principles by which anti-piracy mechanisms will be weighed against and to steer the future development of such mechanisms
    b. Specific objectives and considerations that tangibly reflect these principles
3. Case study to show the framework in action
    a. Graduated response policies
        i. HADOPI law
        ii. "Six strikes" warning system
    b. Lawsuits against individual infringers
4. Meta-analysis of the framework — strengths, weaknesses, possibilities for future improvement
5. Proposition as to how the framework might be used and integrated into debates over anti-piracy legislation and the overall decision-making process

As a starting point, we've identified three broad principles that will serve as the basis of the framework. We believe that they comprehensively cover the major points of contention in assessing anti-piracy policies and should be reasonably satisfactory for all parties. Moreover, we've narrowed down the specific objectives that we'll be investigating to the bare essentials:

1. Is effective in reducing piracy (economic argument)
    a. Ease of circumvention
    b. Revenue in reclaimed sales
    c. Positive effects on employment
2. Has minimal negative repercussions on internet (technical "MIT expertise" argument)
    a. e.g. DNS
    b. Non-infringing use of technology – effects on innovation (e.g. Megaupload, torrents)
    c. Fair use arguments (creative/cultural)
3. Will be acceptable to stakeholders (political/legal argument)
    a. Who will implement? Legal authority/precedents?
    b. Costs of implementation/enforcement
    c. Political views/possible challenges of stakeholders, e.g. industry, citizens, artists

With respect to the economic arguments, we don't expect to be devising an actual equation to plug numbers into. Considering our current level of knowledge and the time frame of the project, this would be impractical. Instead, we will be taking a more broad view of the economic effects that an anti-piracy mechanism might have on sales and employment.

As for technical arguments, these should become more apparent as we delve further into the research. Naturally, we won't be able to go into detail of all the potential technical problems that an anti-piracy mechanism might pose; however, we can identify the broader issues as well as particularly key standards and systems to pay close attention to (e.g. DNS).

In terms of mentorship, we would best be assisted by someone who understands how economic analyses of piracy are conducted as well as the overall political landscape of copyright legislation. Looking at the points identified above, we feel that we can amply address (2), could benefit from support on (3), and definitely require guidance with (1).

so is this our outline

do we list these anywhere?

ie not quant

for our 3 things

Steven 10/23

(Skimmed the paper)

Lit Review

Ob
- Pro
- Con
- Referee

Ov Thoughts

Easily circumventable - still Ok

So what qu to answer

1. Address to
   - Wanted specific office
     - They mentioned one
     - write it down
     - Economic Advisers
2. What's the problem
   - more of political problem
   - legislative process - what to do

(7)

Really discussed last time

3. Possible Sol
   - Framework
   - Graduated Response
   - (one size fits all)

4. Why better
   - more fair + balance
   - validity

   Argue graduated response

(economic analysis on freedom of internet)

5. Arguments against our Sol
   - too mediating
   - ineffective
   - Stakeholders have diff value judgements

6. Proposed bibliography
   - look some up - done
   - write it up

(3)

(Still need to research Hadoop)

Me: Bibliography

Stephen: Will do rest

Do tonight

Assignment due Oct. 24 (on Stellar, one paper per team)

Each team should turn in a complete outline of your report. By complete outline, we mean that you should present the major conclusions of your report and the logic that leads to them. This does not have to be written in polished English, and it can even be in outline form. But it should cover the major content of your report: What you're recommending and how you will support those recommendations. In particular, it should cover:

1. Who is the report addressed to?
2. What's the problem?
3. What are possible solutions?
4. Why is our solution better than other solutions?
5. What are arguments against our solution and how do you repond to them?
6. Proposed bibliography

To help you get oriented, here are some guidelines on writing policy papers. (These pertain to the final paper, not to this draft.)

12/1

Sections

Tech - me

Stakeholders - Stephen

Econ - split

Sections

HADOPI - Steven

6 strikes vs lawsuit - Plaz

Talk more

Read 10/26 plane

FINAL
7/6/2011

MEMORANDUM OF UNDERSTANDING

Whereas:

- Copyright infringement (under Title 17 of the United States Code) on the Internet ("Online Infringement") – including the illegal distribution of copyrighted works such as music, movies, computer software, gaming software, e-books and the like via Peer-to-Peer ("P2P") file exchanges and other illegal distribution via Internet file hosting, streaming or other technologies – imposes substantial costs on copyright holders and the economy each year. Online Infringement also may contribute to network congestion, negatively affecting users' Internet experiences. The availability of copyrighted content, including live and recorded programming, from pirated sources harms legitimate content creation and distribution. Content creators are taking steps to make lawful content more available online. The lawful online distribution businesses are vibrant and growing and they are harmed by infringement. In addition, law enforcement is pursuing opportunities to enhance its ability to investigate, prosecute, and ultimately punish and deter those who violate copyright law.

- While the government maintains a critical role in enforcing copyright law, it should be readily apparent that, in an age of viral, digital online distribution, prosecution of individual acts of infringement may serve a purpose, but standing alone this may not be the only or best solution to addressing Online Infringement. If Online Infringement is to be effectively combated, law enforcement must work with all interested parties, including copyright holders, their licensees, artists (and the guilds, unions and other organizations that represent them), recording companies, movie studios, software developers, electronic publishers, Internet Service Providers ("ISPs"), public interest groups, other intermediaries and consumers on reasonable methods to prevent, detect and deter Online Infringement. Such efforts must respect the legitimate interests of Internet users and subscribers in protecting their privacy and freedom of speech, in accessing legitimate content, and in being able to challenge the accuracy of allegations of Online Infringement. This work should include an educational component because evidence suggests that most informed consumers will choose lawful services and not engage in Online Infringement. This work also should include the development of solutions that are reasonably necessary to effectuate the rights that are granted by copyright without unduly hampering the legitimate distribution of copyrighted works online or impairing the legitimate rights and interests of consumers and ISPs. Such efforts serve not only the shared interests of creators and distributors of creative works, but also the interests of Internet users who benefit from constructive measures aimed at education and deterrence in lieu of litigation with its attendant costs and legal risk.

Poorly written as well

- A reasonable, alert-based approach may help to protect legal rights granted by copyright and stem the unlawful distribution of copyrighted works, while

providing education, privacy protection, fair warning and an opportunity for review that protects the lawful interests of consumers. The efficiencies gained from such a cooperative model may benefit all interested parties, including consumers.

- Enforcement and consumer education programs alone may not be able to fully address the issue of Online Infringement. In addition, it is important for content and copyright owners to continue to make available an array of lawful alternatives for consuming movies, music, and other content online, including new distribution models that make it easy and attractive for consumers to lawfully obtain online the content they want. ISPs can assist in these efforts by encouraging subscribers to seek legal alternatives for obtaining content. The widespread availability of lawful content will benefit consumers, content owners and ISPs.

Whereas, the Content Owner Representatives, the Participating ISPs, and the members of the Participating Content Owners Group (all, as defined in Section 1 below) and independent record labels and film production companies (Independent Content Owners , as defined in Section 5C below) represented by the American Association of Independent Music ("A2IM") and the Independent Film and Television Alliance ("IFTA"), respectively, seek to establish a consumer-focused process for identifying and notifying residential wired Internet access service customers of the Participating ISPs ("Subscribers") (other than dial-up Subscribers) who receive multiple notifications of allegations of Online Infringement made via P2P networks and applications ("P2P Online Infringement"), in an effort to educate consumers, deter Online Infringement, and direct consumers to lawful online legitimate sources of content.

Whereas, having considered the desirability of implementing such a process as a means to encourage lawful and legitimate use of copyrighted content, the Parties (as defined in Section 1 below) hereby voluntarily enter into this Memorandum of Understanding (the "Agreement").

IT IS HEREBY UNDERSTOOD AND AGREED AMONG THE PARTIES THAT:

1. Parties to the Agreement

The parties to this Agreement (the "Parties") are The Recording Industry Association of America, Inc. ("RIAA"), The Motion Picture Association of America, Inc. ("MPAA" and together with RIAA, the "Content Owner Representatives"); the entities set forth in Attachment A (as may be amended from time to time) (collectively, the "Participating ISPs"); and solely for the purposes of Sections 2(E), 4(C), 4(D), 4(H), 4(I), 5(A), 5(C), 6, 7, 8, 9(E), 9(F), and 10 of this Agreement, MPAA members Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc. (such MPAA members, together with MPAA, the "MPAA Group"), RIAA members UMG Recordings, Inc., Warner Music Group, Sony Music

Entertainment, and EMI Music North America (such RIAA members, together with RIAA, the "RIAA Group" and together with the MPAA Group, and any other entities set forth in Attachment B (as may be amended from time to time), the "Participating Content Owners Group").

2. Establishment of CCI

A. Not later than sixty (60) days after the Effective Date (as defined in Section 8(A) below), the Content Owner Representatives and the Participating ISPs will establish the Center for Copyright Information ("CCI") to assist in the effort to combat Online Infringement by, among other things, (i) taking an active role in educating the public about the laws governing the online distribution of works protected by copyright, including educating the public regarding civil and criminal penalties for Online Infringement; (ii) interfacing with third party stakeholders on issues and questions of common interest to the Content Owner Representatives and the Participating ISPs pertaining to Online Infringement and related matters; (iii) assisting in the design and implementation of a process that provides for consumer and Subscriber education through the forwarding of Copyright Alerts to, and application of Mitigation Measures (as defined in Section 4(G)(iii) below) on, Subscribers engaged in persistent P2P Online Infringement, including reviewing the accuracy and efficacy of Content Owner Representative processes for identifying instances of P2P Online Infringement and ISP processes for identifying the Subscriber accounts associated with such P2P Online Infringement; (iv) periodically reviewing the effectiveness and impact of such processes as further described in Section 9 below; (v) collecting and disseminating to interested parties and the public data regarding Online Infringement and the lawful means available to obtain non-infringing copyrighted works; and (vi) facilitating the involvement of non-participating ISPs in the work of CCI and in the Copyright Alert program (as defined in Section 4(G) below).

B. CCI will be governed by a six (6) member executive committee (the "Executive Committee") that will be selected as follows: three (3) members to be designated collectively by the Content Owner Representatives, and three (3) members to be designated collectively by the Participating ISPs. Each member shall serve without compensation for a term of two (2) years, which may be renewed.

C. The members of the Executive Committee shall be selected within forty-five (45) days of the Effective Date (as defined in Section 8(A) below). The Executive Committee shall hold an initial meeting and designate an individual to serve as its Executive Director. The Executive Director shall not be one (1) of the six (6) members of the Executive Committee.

D. The Executive Committee shall also establish a three (3) member advisory board to the Executive Committee (the "Advisory Board"). The Content Owner Representatives shall select one (1) member of the Advisory Board, the Participating ISPs shall select one (1) member of the Advisory Board, and the two (2) selected Advisory Board members shall select the third member. Each of the members of the

Advisory Board shall be drawn from relevant subject matter expert and consumer interest communities and, unless otherwise agreed in writing, shall not be employees or agents of the Content Owner Representatives nor of the Participating ISPs. The Advisory Board shall be consulted on any significant issues the Executive Committee is considering relating to the design and implementation of the Notice Process and the Copyright Alert program (as defined in Section 4(C) and Section 4(G), respectively), and shall provide recommendations to the Executive Committee as appropriate. The Advisory Board may also provide recommendations regarding the CCI educational program described in Section 3 below, upon the Executive Committee's request.

E. Funding for CCI will be provided fifty percent (50%) by the Participating Content Owners Group and fifty percent (50%) by the Participating ISPs. The initial CCI budget shall be presented to and approved by the Executive Committee within ninety (90) days of the Effective Date (as defined in Section 8(A) below) and shall be funded by the Participating Content Owners Group and the Participating ISPs promptly thereafter according to the apportionment set forth in this Section 2(E). The Executive Committee shall also oversee and approve by majority all matters regarding the corporate formation of CCI and the further development of its internal structure. CCI shall be governed by its articles of incorporation and bylaws to be filed in connection with its corporate formation in the State of Delaware. The bylaws shall, inter alia, include a mechanism for adding parties to this Agreement.

3. CCI Educational Program

In conformance with its budget, CCI shall develop an educational program to inform the public about laws prohibiting Online Infringement and lawful means available to obtain digital works online and through other legitimate means. CCI will also establish, host and maintain an online information center where educational material will be available to the general public. The Content Owner Representatives and the Participating ISPs shall contribute to CCI any applicable educational materials already developed by the respective Content Owner Representatives and Participating ISPs, and CCI shall facilitate the dissemination of such educational materials through online or other media. Such educational materials shall include, among other things, information about the technical means Subscribers can use to secure their computers and networks to avoid unwittingly assisting others in Online Infringement. Any Content Owner Representative or Participating ISP may add additional educational materials to the online information center subject to the prior permission of the Executive Committee.

4. System for Reducing Instances of P2P Online Infringement

A. The Content Owner Representatives will develop and maintain written methodologies, which shall be adopted by the applicable Content Owner Representative, for identifying instances of P2P Online Infringement that are designed to detect and provide evidence that the identified content was uploaded or downloaded or copied and offered on a P2P network to be downloaded through a bit torrent or other P2P technology. Each Participating ISP will develop and maintain methodologies, which

shall be adopted by the applicable Participating ISP, to match Internet Protocol ("IP") addresses identified by the Content Owner Representatives to the Participating ISP Subscribers' accounts, to keep a record of repeat alleged infringers, and to apply Mitigation Measures (as defined in Section 4(G)(iii) below). Such Content Owner Representative and Participating ISP methodologies are collectively referred to herein as the "Methodologies". The goal of these Methodologies shall be to ensure that allegations of P2P Online Infringement, related records, and the application of any Mitigation Measures are based on reliable, accurate, and verifiable processes and information.

B. In conformance with its budget, CCI shall retain an independent and impartial technical expert or experts (the "Independent Expert") to review on a periodic and ongoing basis the Methodologies and any modifications thereto, and recommend enhancements as appropriate, with the goal of ensuring and maintaining confidence on the part of the Content Owner Representatives, the Participating ISPs, and the public in the accuracy and security of the Methodologies. If a Content Owner Representative Methodology is found by the Independent Expert to be fundamentally unreliable, the Independent Expert shall issue a confidential finding of inadequacy ("Finding of Inadequacy") to the affected Content Owner Representative to permit the affected Content Owner Representative to modify or change the Methodology for review. The selection of the Independent Expert shall require approval by a majority of the members of the Executive Committee. The Content Owner Representatives and the Participating ISPs agree to provide reasonable cooperation to the Independent Expert and provide to the Independent Expert a copy of their respective Methodologies, and any technical or other information reasonably related to their respective Methodologies needed to undertake this review process. As a condition of retention, the Independent Expert shall agree in writing to keep confidential any proprietary or other confidential information provided by the Content Owner Representatives and the Participating ISPs as part of the Independent Expert's review. The Content Owner Representatives and each Participating ISP shall exchange general descriptions of their respective Methodologies upon request. At the direction of CCI, the Independent Expert may consult with each Content Owner Representative or Participating ISP concerning the implementation and ongoing operation of that Representative's or ISP's Methodology. In addition, the Independent Expert will (i) review the Methodologies with recognized privacy experts agreed to by a majority of the Executive Committee and (ii) recommend enhancements to the Methodologies as appropriate to address privacy issues, if any, identified by the privacy experts. Failure to adopt a recommendation of the Independent Expert shall not amount to a breach under this Agreement. The Independent Expert's recommendations must be shared with each of the Content Owner Representatives and the affected Participating ISP, but may not be disclosed to other parties, including Participating ISPs other than the affected Participating ISP, without the express written permission of each Content Owner Representative and the affected Participating ISP and any disclosure to such other third parties shall not include any proprietary or otherwise confidential information of the Content Owner Representative(s) or Participating ISP affected.

C. The Content Owner Representatives may send notices pursuant to this Agreement and the implementation agreements described in Section 5(A) of this

Agreement (the "Implementation Agreements") to the Participating ISPs of instances of alleged P2P Online Infringement (each an "ISP Notice"), and the Participating ISPs shall accept and process such notices involving the Participating ISPs' Subscribers (such Content Owner Representative and Participating ISP actions being, together, a "Notice Process"). The Content Owner Representatives agree to generate ISP Notices only for instances of P2P Online Infringement identified through the use of the Content Owner Representative Methodologies that have been reviewed and evaluated by the Independent Expert, and that have not been issued a Finding of Inadequacy. For purposes of generating ISP Notices, the Content Owner Representatives further agree to focus on instances of P2P Online Infringement involving files or data consisting primarily of infringing material or containing unauthorized copyrighted works in complete or substantially complete form and to avoid instances of P2P activity in which *de minimis* amounts of allegedly infringing material are incorporated into files or data consisting primarily of non-infringing material. The Content Owner Representatives will also endeavor to generally send the ISP Notices within twenty-four (24) hours of confirmed identification of the alleged activity described in the ISP Notice. ISP Notices shall be generated and sent solely by the Content Owner Representatives or their service providers (including on behalf of the Participating Content Owners Group, the Independent Content Owners (as defined in Section 5(C) below), the RIAA Group's members' distributed labels and those entities set forth in Attachment D hereto). The individual members of the Participating Content Owners Group; IFTA and A2IM; the Independent Content Owners (as defined in Section 5(C) below); the RIAA Group's members' distributed labels; and those entities set forth in Attachment D hereto shall not generate or send ISP Notices.

D. The Content Owner Representatives agree that each ISP Notice provided to a Participating ISP as part of the Notice Process shall clearly identify: (i) the copyrighted work that allegedly has been infringed and the owner of such work; (ii) a description of the basis upon which the notifying Content Owner Representative or its agent asserts the right to enforce the particular affected copyright on behalf of the person or entity who owns or controls the copyright and/or exclusive distribution rights in the copyright (a "Copyright Owner"); (iii) a statement that the notifying Content Owner Representative or its agent has a good faith belief that use of the material is not authorized by the Copyright Owner, its agent, or the law; (iv) a statement that the information in the ISP Notice is accurate and that, under penalty of perjury, the Content Owner Representative is authorized to act on behalf of the Copyright Owner whose rights were allegedly infringed; and (v) technical information necessary for the Participating ISP to identify the Subscriber (*e.g.*, IP address, date, time and time zone of the alleged P2P Online Infringement, and such additional information as may be necessary as the Participating ISPs transition to IPv6). The Content Owner Representatives and the Participating Content Owners Group agree that all notices of P2P Online Infringement generated by them or on their behalf and delivered to the Participating ISPs shall meet the requirements for ISP Notices hereunder, shall comply with the terms hereof and shall be governed exclusively by this Agreement and the Implementation Agreements.

E. Reserved.

F. Each Participating ISP agrees to communicate the following principles in its Acceptable Use Policies ("AUP") or Terms of Service ("TOS"): (i) copyright infringement is conduct that violates the Participating ISP's AUP or TOS and for which a Subscriber may be legally liable; (ii) continuing and subsequent receipt of Copyright Alerts (as defined in Section 4(G) below) may result in the Participating ISP taking action by the application of Mitigation Measures (as defined in Section 4(G)(iii) below); and (iii) in addition to these Mitigation Measures, the Participating ISP may also adopt, in appropriate circumstances, those measures specifically authorized by section 512 of the Digital Millennium Copyright Act ("DMCA") and/or actions specifically provided for in the Participating ISP's AUP and/or TOS including temporary suspension or termination, except that nothing in this Agreement alters, expands, or otherwise affects any Participating ISP's rights or obligations under the DMCA.

G. Each Participating ISP will develop, implement and independently enforce a Copyright Alert program as described in this Section 4(G) (each such program a "Copyright Alert Program"), provided that each Participating ISP shall not be required to exceed the notice volumes pertaining to its Copyright Alert Program as established in Section 5 of this Agreement. Each Participating ISP's Copyright Alert Program will be triggered by the Participating ISP's receipt of an ISP Notice that can be associated with a Subscriber's account and will result in the Participating ISP sending one (1) or more alert notices to the applicable Subscriber concerning the ISP Notice, as further described below (each such alert notice a "Copyright Alert").

Each Participating ISP's Copyright Alert Program shall be comprised of six (6) Copyright Alerts, except that a Participating ISP may elect to send a single Educational Step Copyright Alert (as defined in Section 4(G)(i) below). However, to give an affected Subscriber time to review each Copyright Alert pertaining to such Subscriber's account and to take appropriate steps to avoid receipt of further Copyright Alerts, a Participating ISP and its Subscriber will be afforded a grace period of seven (7) calendar days after the transmission of any Copyright Alert before any additional Copyright Alerts will be directed to the account holder (the "Grace Period"). The same Grace Period shall apply following the sending of a Mitigation Measure Copyright Alert (as described in Section 4(G)(iii) and (iv) below) and during the pendency of any review requested by a Subscriber following the receipt of either such Copyright Alert. During such Grace Period, any further ISP Notices received by the Participating ISP that the Participating ISP determines to be associated with the applicable Subscriber's account will be handled as described in sub-paragraphs (i), (ii), (iii), and (iv) below.

Each Participating ISP shall use commercially reasonable efforts to develop a Copyright Alert Program in accordance with this Section 4(G), and shall work in good faith to complete all technical development work necessary for implementation of its Copyright Alert Program by a target launch date set forth in the applicable Implementation Agreement (each Participating ISP's target launch date referred to herein as its "Copyright Alert Program Launch Date").

Each Participating ISP's Copyright Alert Program shall be substantially similar to the following four (4) step sequential framework, which shall include an educational step (the "Initial Educational Step"), an acknowledgement step (the "Acknowledgement Step"), a mitigation measures step (the "Mitigation Measures Step"), and a post mitigation measures step (the "Post Mitigation Measures Step") as further described below. Under this framework, each Participating ISP will send Copyright Alerts with escalating warning language to Subscribers who are the subject of continuing ISP Notices. Specifically, each Participating ISP (1) shall send the Subscriber up to two (2) Copyright Alerts during the Initial Educational Step; (2) shall send two (2) more Copyright Alerts during the Acknowledgement Step; (3) shall send one (1) Mitigation Measure Copyright Alert (as defined in Section 4(G)(iii) below) during the Mitigation Measures Step and shall apply the specified Mitigation Measure (as defined in Section 4(G)(iii) below), subject to the Subscriber's right to challenge (or the Participating ISP's discretion to waive) the Copyright Alert(s) at this step; and (4) during the Post Mitigation Measures Step, shall send one (1) Mitigation Measure Copyright Alert and shall apply the specified Mitigation Measure, and may, at the Participating ISP's sole discretion, send additional Mitigation Measure Copyright Alerts and apply additional Mitigation Measures, subject to the Subscriber's right to challenge Copyright Alerts at this step.

Each Participating ISP's Copyright Alert Program shall follow the following format:

(i) Initial Educational Step: Upon receipt of an ISP Notice associated with a Subscriber's account and taking into account the parameters of the Grace Period (if applicable), the Participating ISP shall direct a Copyright Alert to the account holder (an "Educational Step Copyright Alert"). The Educational Step Copyright Alert shall notify the Subscriber of receipt of an ISP Notice alleging P2P Online Infringement and shall include, at a minimum, the information contained in the ISP Notice regarding the alleged infringement and shall inform the Subscriber that: (a) copyright infringement is illegal as well as a violation of the Participating ISP's AUP or TOS, (b) users of the Subscriber's account must not infringe copyrighted works, (c) there are lawful methods of obtaining copyrighted works, (d) continuing and subsequent receipt of Copyright Alerts may result in the Participating ISP taking action by the application of Mitigation Measures, (e) in addition to these Mitigation Measures, the Participating ISP may also adopt, in appropriate circumstances, those measures specifically authorized by section 512 of the DMCA and/or actions specifically provided for in the Participating ISP's AUP and/or

TOS including temporary suspension or termination,[1/] (f) the Subscriber will have an opportunity to challenge any Copyright Alerts associated with the Subscriber's account before a Mitigation Measure is applied and may therefore wish to preserve records or information that could be used to show that the Subscriber's conduct was non-infringing, and (g) additional information regarding the Copyright Alert program may be found at CCI's web site. The number of Educational Step Copyright Alerts shall be at the discretion of the Participating ISP, not to exceed two (2) Copyright Alerts per Subscriber account, taking into account the parameters of the Grace Period. The second Educational Step Copyright Alert shall note specifically that it is in fact the Subscriber's second Educational Step Copyright Alert.

If the Participating ISP receives one (1) or more additional ISP Notices attributable to such Subscriber's account during the Grace Period associated with one of the Educational Step Copyright Alerts, the Participating ISP may at its discretion emphasize the educational and warning nature of its Copyright Alert Program by directing to the account holder additional Copyright Alerts that are similar in style to the Educational Step Copyright Alert. Such supplemental Copyright Alerts sent during the Grace Period shall not count toward the limit of two (2) Educational Step Copyright Alerts.

(ii) Acknowledgement Step: At the Acknowledgement Step, upon receipt of further ISP Notices determined to be associated with a Subscriber's account and taking into account the parameters of the Grace Period, the Participating ISP shall direct two (2) Copyright

---

1/ The Parties acknowledge and agree that the limitations on ISP liability under the DMCA are conditioned on an ISP's adoption and reasonable implementation of a policy that provides for the termination in appropriate circumstances of subscribers and account holders who are repeat infringers ("DMCA Termination Policy"). Notwithstanding the foregoing, (1) this Agreement does not and is not intended to create any obligation on a Participating ISP to adopt, implement, enforce, or otherwise take any action in furtherance of a DMCA Termination Policy; (2) the adoption, implementation, enforcement, or other action in furtherance of a DMCA Termination Policy is not part of any step of the Copyright Alert program or enforceable under this Agreement; and (3) entering into this Agreement is not, by itself, intended to address whether a Participating ISP has adopted and reasonably implemented a DMCA Termination Policy. This Agreement does not and is not intended to establish any legal inference regarding any ISP that does not participate in the Copyright Alert program or to address whether or not any ISP has adopted and reasonably implemented a DMCA Termination Policy. All references in this Agreement to the possibility of termination of a subscriber account are intended solely as an informational element of the Copyright Alerts required by the Copyright Alert program.

Alerts to the account holder that, as further described below, will require acknowledgement of receipt (but not require the user to acknowledge participation in any allegedly infringing activity) (each such Copyright Alert an "Acknowledgement Step Copyright Alert"). Each such Acknowledgement Step Copyright Alert shall state that the Subscriber, by acknowledging the notice, agrees immediately to cease, and/or agrees to instruct other users of the Subscriber's account to cease infringing conduct, if any exists. Each such Copyright Alert shall also state that, upon receipt of lawful process requiring production of records or pursuant to a qualifying claim that the Subscriber has made via the Independent Review Program (as defined in Section 4(H) below and Attachment C hereto), the Participating ISP may provide relevant identifying information about the Subscriber and the Subscriber's infringing conduct to third parties, including Content Owner Representatives or their agents and law enforcement agencies.

The mechanism provided for the Subscriber to acknowledge an Acknowledgement Step Copyright Alert may be in the form of (a) a temporary landing page to which the Subscriber's browser is directed prior to permitting general access to the Internet ("Landing Page") that shall state that the Subscriber has received prior warnings regarding P2P Online Infringement, and shall require the user of the Subscriber's account to acknowledge receipt by clicking through the page prior to accessing additional web pages, (b) a "pop-up" notice which shall be designed to persist until the user of the Subscriber's account acknowledges receipt by clicking through the pop-up notice, or (c) such other format as determined in the Participating ISP's reasonable judgment which shall require acknowledgement of receipt of the Acknowledgement Step Copyright Alert.

If the Participating ISP receives one (1) or more additional ISP Notices attributable to such Subscriber's account during the Grace Period associated with one of the Acknowledgement Step Copyright Alerts, the Participating ISP may at its discretion emphasize the educational and warning nature of its Copyright Alert Program by directing to the account holder additional Copyright Alerts that are similar in style to the Educational Step Copyright Alert or the Acknowledgement Step Copyright Alert. Such supplemental Copyright Alerts sent during the Grace Period shall not count toward the limit of two (2) Acknowledgement Step Copyright Alerts.

(iii) Mitigation Measures Step: At the Mitigation Measures Step, upon receipt of further ISP Notices determined to be associated with a

Subscriber's account and taking into account the parameters of the Grace Period, the Participating ISP shall direct a Copyright Alert (a "Mitigation Measure Copyright Alert") to the account holder that (a) requires acknowledgement of receipt of the Copyright Alert as described in the Acknowledgement Step, (b) shall state that the Subscriber has received prior warnings regarding alleged P2P Online Infringement, and (c) informs the Subscriber that, per the Participating ISP's AUP and/or TOS and as set forth in prior Copyright Alerts, additional consequences shall be applied upon the Subscriber's account as described more fully in this subparagraph (iii) (each such measure a "Mitigation Measure").

The Mitigation Measure Copyright Alert shall set forth the specific Mitigation Measure to be applied and shall inform the Subscriber that, unless the Subscriber has requested review under one of the dispute resolution mechanisms specified in Section 4(H) below, the Participating ISP shall apply the selected Mitigation Measure after the expiration of a notice period of ten (10) business days or fourteen (14) calendar days from the time the Mitigation Measure Copyright Alert is delivered. The term of the notice period (*i.e.*, ten (10) business days or fourteen (14) calendar days) shall be at the Participating ISP's discretion. If no review is requested by the Subscriber, the Participating ISP shall apply the specified Mitigation Measure on the applicable Subscriber's Internet access service account after such ten (10) business day or fourteen (14) calendar day period has expired.

The Mitigation Measure applied at the Mitigation Measures Step shall be one of the following, determined by the Participating ISP and applied in a manner reasonably calculated, in the Participating ISP's reasonable discretion, to help deter P2P Online Infringement: (a) temporary reduction in uploading and/or downloading transmission speeds; (b) temporary step-down in the Subscriber's service tier to (1) the lowest tier of Internet access service above dial-up service that the Participating ISP makes widely available to residential customers in the Subscriber's community, or (2) an alternative bandwidth throughput rate low enough to significantly impact a Subscriber's broadband Internet access service (*e.g.*, 256 - 640 kbps); (c) temporary redirection to a Landing Page until the Subscriber contacts the Participating ISP to discuss with it the Copyright Alerts; (d) temporary restriction of the Subscriber's Internet access for some reasonable period of time as determined in the Participating ISP's discretion; (e) temporary redirection to a Landing Page for completion of a meaningful educational instruction on copyright; or (f) such other temporary Mitigation Measure as may be applied by the Participating ISP in its

discretion that is designed to be comparable to those Mitigation Measures described above. Participating ISPs shall not be obligated to apply a Mitigation Measure that knowingly disables or is reasonably likely to disable a Subscriber's access to any IP voice service (including over-the-top IP voice service), e-mail account, or any security service, multichannel video programming distribution service or guide, or health service (such as home security or medical monitoring) while a Mitigation Measure is in effect.

The foregoing provisions notwithstanding, the Participating ISP will retain the discretion, on a per Subscriber account basis, (a) to decide whether appropriate circumstances exist to waive such Mitigation Measure (a "Waiver"), provided that the Participating ISP will only issue one (1) such Waiver per Subscriber account, or (b) instead of applying the Mitigation Measure specified in the Mitigation Measure Copyright Alert, to apply an alternate Mitigation Measure on the Subscriber's Internet access service account and to so inform the Subscriber.

If the Participating ISP elects to use a Waiver, the Participating ISP will direct to the account holder a final warning (a "Fifth Warning Copyright Alert") that will contain each of the elements contained in the Mitigation Measure Copyright Alert as described in this Section 4(G)(iii) and will inform the Subscriber that, in the event that the Participating ISP receives one (1) or more further ISP Notices from a Content Owner Representative, the Subscriber's Internet access service account will be subject to a Mitigation Measure per the Participating ISP's AUP and/or TOS and as set forth in prior Copyright Alerts, unless the Subscriber requests review under one of the dispute resolution mechanisms specified in Section 4(H). If, after the expiration of the Grace Period following issuance of a Fifth Warning Copyright Alert, a Participating ISP receives one (1) or more further ISP Notices determined to be related to a Subscriber's account for which a Waiver has been granted, the Participating ISP will proceed with the transmission of a Mitigation Measure Copyright Alert and the associated activities described above.

(iv) Post Mitigation Measures Step: In the event that a Participating ISP receives a further ISP Notice determined to be associated with a Subscriber's account after a Mitigation Measure has been applied on that Subscriber's account, the Participating ISP shall direct a further Mitigation Measure Copyright Alert to the account holder and after ten (10) business days or fourteen (14) calendar days, as applicable, either re-apply the previous Mitigation Measure or

apply a different Mitigation Measure, unless the Subscriber requests review under one of the dispute resolution mechanisms specified in Section 4(H). The Mitigation Measure Copyright Alert at this step shall also inform the Subscriber that the Subscriber may be subject to a lawsuit for copyright infringement by the Copyright Owners and that continued infringement may, in appropriate circumstances, result in the imposition of action consistent with section 512 of the DMCA and/or actions specifically provided for in the Participating ISP's AUP and/or TOS including temporary suspension or termination. Upon completion of the Post Mitigation Measures Step, a Participating ISP may elect voluntarily to continue forwarding ISP Notices received for that Subscriber account, but is not obligated to do so. The Participating ISP will, however, continue to track and report the number of ISP Notices the Participating ISP receives for that Subscriber's account, so that information is available to a Content Owner Representative if it elects to initiate a copyright infringement action against that Subscriber.

(v) Reset: If a Participating ISP does not receive an ISP Notice relating to a Subscriber's account within twelve (12) months from the date the Participating ISP last received an ISP Notice relating to that same Subscriber's account, (a) the next ISP Notice associated with that Subscriber's account shall be treated as the first such ISP Notice under the provisions of this Copyright Alert Program and the Subscriber may be afforded an additional Waiver as set forth in Section 4(G)(iii) above; and (b) the Participating ISP may expunge all prior ISP Notices and Copyright Alerts from the Subscriber's account.

(vi) Transmission of Copyright Alerts to Subscribers: Copyright Alerts should be directed by the Participating ISP to the account holder by means that are designed to ensure prompt receipt (*e.g.*, via email, physical mail, auto-dialer notification, ISP account management tool pop-ups requiring user click through, electronic or voice communications with Subscribers or such other means of delivery as the Participating ISP deems commercially practicable), and the Participating ISP shall design such Copyright Alerts in a manner reasonably calculated, in the Participating ISP's discretion, to be received by the Subscriber. Each Copyright Alert after the initial Educational Step Copyright Alert will include the educational and general information required in the Educational Step Copyright Alert and in any other Copyright Alerts that were forwarded to the Subscriber after the Educational Step, together with a summary of the pertinent information regarding the alleged P2P Online Infringement related to prior ISP Notices or a link or

other mechanism by which the Subscriber can access or obtain such information. Each Participating ISP will provide the form of its Copyright Alerts to the Independent Expert as part of the Independent Expert's review of each Participating ISP's Methodology, and will in good faith consider any suggestions from the Independent Expert.

(vii) Notification of Ability to Request Review: Copyright Alerts directed to account holders at the Mitigation Measures Step and the Post Mitigation Measures Step shall inform the Subscriber of the Subscriber's ability to request review within ten (10) business days or fourteen (14) calendar days, as applicable, under one of the dispute resolution mechanisms described in Section 4(H). If the Subscriber requests such review, the Participating ISP shall, upon receiving notice of the request for such review and pending a final decision via the chosen dispute resolution mechanism, defer taking any further action under its Copyright Alert Program.

H. Independent Review Program

(i) A Subscriber may seek review of a Mitigation Measure Copyright Alert via the dispute resolution program set forth in Attachment C (the "Independent Review Program") or as otherwise permitted in the Participating ISP's AUP or TOS or as permitted by law, at the election of the Subscriber. The Independent Review Program shall allow for the Subscriber to remain anonymous to the Content Owner Representatives and the members of the Participating Content Owners Group, except in cases where the Subscriber elects a defense in which the Subscriber's identity will be disclosed. The decision from the Independent Review Program shall be binding on the Parties solely for purposes of the Notice Process and the affected Copyright Alert Program but shall have no force or effect beyond the Notice Process and the affected Copyright Alert Program, and shall not be deemed to adjudicate any rights outside of this limited context. In any judicial proceeding between a Subscriber and a Copyright Owner concerning subject matter that is or has been the subject of the Independent Review Program, as provided in the procedures governing the Independent Review Program, neither the Subscriber nor the Copyright Owner shall seek to enter into evidence, or otherwise refer to or cite, either the fact of the Independent Review or any outcome of the Independent Review.

(ii) The costs of establishing and administering the Independent Review Program shall be borne fifty percent (50%) by the Participating Content Owners Group and fifty percent (50%) by the Participating ISPs.

I. Generation of Monthly Reports

Within ten (10) business days of the end of each calendar month during the term of this Agreement, each Participating ISP shall provide reporting of non-personally

identifiable information to the Content Owner Representatives identifying, on an anonymized basis and in the format set forth in the Participating ISP's Implementation Agreement, information about those Subscribers who have received Copyright Alert(s) during the applicable calendar month and the total number of alleged P2P Online Infringements by each such Subscriber. Such reporting may be done via Automated Copyright Notification System ("ACNS") standards or other available methods as mutually agreed in the Participating ISP's Implementation Agreement. The Parties may not (i) use or disclose such data to governmental entities (absent lawful process) or other third parties, unless prior approval for each such use or disclosure is received from a majority of the CCI Executive Committee and the data is disclosed only on an aggregated, anonymized basis, or (ii) use such reports or any of the data that is included in or may be extrapolated from such reports to attempt to obtain the identity of a Subscriber; except that (1) the Parties may use the reports or data to analyze the effectiveness of the Copyright Alert program; and (2) the Content Owner Representatives or any other member of the Participating Content Owners Group may use such reports or data as the basis for seeking a Subscriber's identity through a subpoena or order or other lawful process. For the avoidance of doubt, the Parties agree that the Content Owner Representatives may share such reports with the other members of the Participating Content Owners Group, provided such Parties agree to abide by the limitations set forth in this Section 4(I).

5. Technical Operations; Implementation Agreements

A. The Content Owner Representatives and each Participating ISP (and the members of the Participating Content Owners Group, as necessary) will work together in good faith to establish and agree upon standardized forms and procedures for a Notice Process (for example, by incorporating ACNS or other mutually agreeable standard(s), and endeavoring to include identification of Methodologies used, if practical). The foregoing sentence notwithstanding, the Parties acknowledge that a common interface between the Content Owner Representatives and the Participating ISPs may not be technically or financially practical. The Content Owner Representatives and each Participating ISP (and the members of the Participating Content Owners Group, as necessary) will document the standards contemplated in this Section 5(A), notice volumes, and other pertinent details concerning the technical operation of the Notice Process and Copyright Alert Program between the Content Owner Representatives and the applicable Participating ISP in an Implementation Agreement. The Content Owner Representatives and the Participating ISPs shall agree to a form of the Implementation Agreement, including the terms and conditions of such agreement, that shall be used by all of the Participating ISPs. Each Participating ISP and the Content Owner Representatives (and the members of the Participating Content Owners Group, as necessary) shall make reasonable efforts to execute their Implementation Agreement no later than three (3) months after the Effective Date (as defined in Section 8(A) below).

B. Reserved.

C. The MPAA Group and the RIAA Group will allocate the number of ISP Notices that each shall be entitled to send to each Participating ISP per month (i) on behalf of their members, the RIAA Group's members' distributed labels, and those entities set forth in Attachment D hereto; and (ii) on behalf of independent record labels and film production companies that are members of the American Association of Independent Music ("A2IM") and the Independent Film and Television Alliance ("IFTA"), respectively (collectively, the "Independent Content Owners"), provided that IFTA, A2IM, and the Independent Content Owners (as applicable) agree to be bound by written agreement (for so long as such agreement remains in effect) to the terms set forth in Sections 4(C), 4(D), 4(H)(i), 4(I), 5(A), 5(C), 6, 7, 8, 9(E), 9(F), and 10 of this Agreement that apply to all members of the Participating Content Owners Group (collectively or individually) and certain designated provisions of each Participating ISP's Implementation Agreement as set forth therein.

D. Each Participating ISP may temporarily cease processing ISP Notices or reduce the number of ISP Notices being processed if, in the sole discretion of the Participating ISP, (i) the Participating ISP receives more ISP Notices than its business processes and systems can reasonably address, (ii) the Participating ISP receives more calls from Subscribers regarding Copyright Alerts than its designated customer service representatives can reasonably address (taking into account the other demands on Participating ISP customer service representatives for unrelated purposes), or (iii) other demands on the Participating ISP's business processes and systems, such as requests from law enforcement, must be given precedence. If the Participating ISP temporarily ceases processing ISP Notices for any of the foregoing reasons, the Participating ISP shall promptly notify the Content Owner Representatives, subject to any limitations on such notice as may be imposed in law or regulation, and shall work cooperatively with the Content Owner Representatives and, if agreed by all affected Parties, the Independent Expert, to resolve any issues relating to the over-provisioning of ISP Notices.

6. Consent to Receive Notices

A. Entry into this Agreement by a Participating ISP shall constitute consent by that Participating ISP to receive ISP Notices from the Content Owner Representatives (or their service providers) on behalf of the Participating Content Owners Group, those entities set forth in Attachment D (as such attachment may be amended from time to time) (or in the case of the RIAA Group, on behalf of the RIAA Group's members' distributed labels), and the Independent Content Owners upon implementation by the Participating ISP of its Copyright Alert Program, subject to all of the terms and limitations set forth in this Agreement and the Participating ISP's Implementation Agreement. The members of the Participating Content Owners Group may change from time to time upon mutual written agreement of the Parties, provided that MPAA and RIAA shall remain Parties to this Agreement and, provided further, that in no event shall such changes increase the notice volumes applicable to each Participating ISP under this Agreement and each Participating ISP's Implementation Agreement, unless this Agreement or the Participating ISP's Implementation Agreement is modified with the

written consent of the Participating ISP to increase the number of ISP Notices that may be sent. Nothing in this Agreement shall require a Participating ISP to accept notices from any third party or restrain it from doing so. No ISP Notices or other notices of P2P Online Infringement directed to Subscribers shall be sent to the Participating ISP by or on behalf of the members of the Participating Content Owners Group, the Independent Content Owners, and those entities set forth in Attachment D of this Agreement (as such attachment may be amended from time to time) (or in the case of the RIAA Group, on behalf of the RIAA Group's members' distributed labels) except pursuant to this Agreement and the Participating ISP's Implementation Agreement.

B. Prior to the Copyright Alert Program launch date for the applicable Participating ISP, such Participating ISP shall continue to process notices concerning P2P Online Infringement in accordance with such Participating ISP's then current policies or practices or, if applicable, agreements with any member of the Participating Content Owners Group.

7. Force Majeure

No Party shall be liable to any other Party for any delay, failure in performance, loss or damage due to fire, explosion, interruption of power supplies, earthquake, flood, the elements, strike, embargo, labor disputes, failure of public transit or other public infrastructure, acts of civil or military authority, war, terrorism, acts of God, acts of the public enemy, acts or omissions of carriers or suppliers, acts of regulatory or governmental agencies, or other causes beyond such Party's reasonable control, whether or not similar to the foregoing and whether or not the Parties contemplate such circumstances at the time of entering into this Agreement.

8. Term; Withdrawal

A. This Agreement shall become effective upon the date all of the Parties have executed this Agreement (the "Effective Date"). This Agreement shall remain in effect for a period of four (4) years following the Effective Date.

B. Any Party may withdraw as a Party from this Agreement prior to its expiration (i) if such Party reasonably determines that continued participation in this Agreement is not technically, commercially, operationally or otherwise practical; (ii) if such Party is subject to a complaint before any administrative agency, court, or other governmental entity challenging the lawfulness of the Copyright Alert program, a Participating ISP's Copyright Alert Program, the Agreement, or an Implementation Agreement to which it is a party or any conduct taken under such agreements or programs; (iii) if another Party to this Agreement is subject to a complaint before any administrative agency, court, or other governmental entity challenging the lawfulness of the Copyright Alert program, a Participating ISP's Copyright Alert Program, or the Agreement or any conduct taken under such agreements or programs; or (iv) if a government entity enacts or establishes a government-sponsored program or judicial, administrative, or executive process concerning P2P Online Infringement that imposes

materially different obligations than those set forth in this Agreement.

9. Records and Evaluation

A. Consistent with its general policies and business practices for retaining Internet access service subscriber records, each Participating ISP agrees to keep reasonable records pertaining to its Copyright Alert Program. Each Participating ISP also agrees to use reasonable efforts to provide semi-annual reports to CCI of the results of its Copyright Alert Program, which shall include, in an aggregated, anonymized form, non-personally identifiable information regarding the ISP Notices received and Copyright Alerts sent and such other aggregated, anonymized data as the Participating ISPs may from time to time agree to provide.

B. Consistent with its general policies and business practices for retaining records regarding Online Infringement, each Content Owner Representative agrees to keep reasonable records pertaining to its participation in the Notice Process under this Agreement including records of the Methodology(ies) currently and previously in use and the effective date(s) of such use. Each Content Owner Representative agrees to use reasonable efforts to provide semi-annual reports to CCI of the results of its Notice Process, which shall include, in an aggregated, anonymized form, non-personally identifiable information regarding the ISP Notices sent to the Participating ISPs concerning activities relating to P2P Online Infringement by the Participating ISPs' Subscribers and such other aggregated, anonymized data as the Content Owner Representatives may from time to time agree to provide. Such reports shall be in a form to be determined by each Content Owner Representative in its discretion.

C. CCI shall keep confidential all records and data relating to the Notice Process and Copyright Alert Programs. None of the records and data relating to the Notice Process and Copyright Alert Programs shall be made publicly available by CCI without prior approval by a majority of the Executive Committee.

D. CCI shall review on an annual basis, beginning on the twelve (12) month anniversary of the Effective Date and occurring each subsequent year thereafter on the anniversary of the Effective Date, the number of Copyright Alerts sent by the Participating ISPs to each Subscriber's account at each step of the Copyright Alert Programs. Based on the information that CCI receives from the Participating ISPs and the Content Owner Representatives, pursuant to Sections 9(A) and 9(B), in order to assess the effectiveness of the Copyright Alert program, CCI shall assess among other things (i) the proportion of Subscribers of each Participating ISP who ceased receiving Copyright Alerts at each step of the Copyright Alert Program; (ii) the average overall number of P2P Online Infringements detected for Content Owner Representative assets over a weekly or monthly period (in general, and by Participating ISP); (iii) the number of ISP Notices received and the number of corresponding Copyright Alerts sent; (iv) the number and percentage of individual Subscribers who, after receiving one (1) or more Copyright Alerts, did not receive additional Copyright Alerts corresponding to their accounts (in general, and by Participating ISP); (v) the number of Subscribers who

requested a review under the Independent Review Program, and at what step they requested it; and (vi) the number and percentage of Independent Reviews which resulted in a decision in favor of the Subscriber – and why such decisions were made. As part of its annual review, CCI shall also examine whether Copyright Alerts are successfully reaching account holders. The Parties shall consider in good faith any recommendations made by CCI resulting from such review and assessment.

E. The Content Owner Representatives, those members of the Participating Content Owners Group and Independent Content Owners selected by the Content Owner Representatives, and the Participating ISPs shall establish a working group under the auspices of CCI, which will consist of appropriate representatives of each Party, who will meet regularly (at least quarterly during the eighteen (18) months following the Effective Date and then at least semi-annually thereafter) to assist in the initiation and implementation of this Agreement, assess its ongoing operation, and thereafter recommend to the Parties on a non-binding basis any suggested amendments to this Agreement to improve its scope or effectiveness. The working group may consult with the Independent Expert as appropriate.

F. CCI shall maintain any reports or other information provided by any Party hereunder in the strictest confidence and shall not disclose such reports or information to any third party or any Party other than the Party which originated the report or information, absent written consent from the originating Party or as otherwise required by law. In the event CCI receives a subpoena or other legal process seeking the disclosure of such reports or information, CCI shall immediately notify the Party whose reports or information is subject to the subpoena or other legal process and provide such Party with the opportunity to seek a protective order or otherwise to oppose disclosure. If authorized by the Executive Committee, CCI shall also seek a protective order or oppose disclosure.

10. Miscellaneous

A. The Content Owner Representatives, the members of the Participating Content Owners Group, the Independent Content Owners, and the Participating ISPs appreciate that alternatives to obtaining and sharing music, movies, and other copyright-protected works by means other than unlawful digital distribution should be encouraged. The Content Owner Representatives will undertake appropriate efforts to ensure the widespread communication of lawful alternatives for consuming content through online distribution methods and encourage the public to utilize these alternatives. Each Participating ISP will, via Copyright Alerts and other avenues, encourage Subscribers to seek legal alternatives to obtain copyrighted materials.

B. This Agreement shall be governed by the laws of the State of New York, without regard to any conflict of law principles. The Parties hereby consent to the exclusive jurisdiction of any state or federal court sitting in the Borough of Manhattan, New York over any judicial proceedings arising out of or related to this Agreement and agree that all claims in respect of such judicial proceedings shall be heard in such state or

federal courts in the Borough of Manhattan, New York. The Parties further agree that any such proceeding shall be filed in the United States District Court for the Southern District of New York if such court has jurisdiction over the proceeding.

C. Nothing expressed or implied in this Agreement is intended, or may be construed, to confer upon or give any person or entity other than the Parties hereto any rights or remedies hereunder. This Agreement may only be amended by written agreement signed by all Parties hereto.

D. This Agreement is subject to any laws or regulations that may be enacted by Congress or adopted by the Federal Communications Commission (or any other federal or state administrative, regulatory or legislative body). If any future law or regulation makes unlawful any provision of this Agreement, that provision will be severed from this Agreement. If any Participating ISP, Content Owner Representative, or member of the Participating Content Owners Group reasonably concludes that such invalidated provision is material to the Agreement or that severing such provision is otherwise impracticable, such Party may immediately terminate its participation in the Agreement.

E. Headings herein are for convenience of reference only and shall in no way affect interpretation of this Agreement.

F. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all proposals, oral or written, all negotiations, conversations or discussions, and all past dealings or industry customs between the parties relating to the subject matter hereof.

G. This Agreement may be executed in two or more counterparts and duplicate originals, each of which will be deemed an original and all of which together will constitute one and the same instrument. An executed copy of this Agreement transmitted via facsimile or email by the executing party and received via facsimile or email by the other party shall have the same legal force as an executed original version of this Agreement.

H. The waiver by a party of any breach of this Agreement by the other party in a particular instance shall not operate as a waiver of subsequent breaches of the same or different kind. Failure of a party to exercise any rights under this Agreement in a particular instance shall not operate as a waiver of such party's right to exercise the same or different rights in subsequent instances.

[The rest of this page is intentionally left blank.]

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By:_____
Name:_____
Title:_____

The Recording Industry Association of America, Inc.

By:_____
Name:_____
Title:_____

Walt Disney Studios Motion Pictures

By:_____
Name:_____
Title:_____

Who for each?

Paramount Pictures Corporation

By:_____
Name:_____
Title:_____

Sony Pictures Entertainment Inc.

By:_____
Name:_____
Title:_____

Twentieth Century Fox Film Corporation

By:_____
Name:_____
Title:_____

Universal City Studios LLC

By:_____
Name:_____
Title:_____

Warner Bros. Entertainment Inc.

By:_____
Name:_____
Title:_____

UMG Recordings, Inc.

By:_____
Name:_____
Title:_____

Warner Music Group

By:_____
Name:_____
Title:_____

Sony Music Entertainment

By:_____
Name:_____
Title:_____

EMI Music North America

By:_____
Name:_____
Title:_____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By:_____
Name:_____
Title:_____

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies)

By:_____
Name:_____
Title:_____

Comcast Cable Communications Management, LLC

By:_____
Name:_____
Title:_____

CSC Holdings, LLC

By:_____
Name:_____
Title:_____

Time Warner Cable Inc.

By:_____
Name:_____
Title:_____

Attachment A – Participating ISPs

The Participating ISPs are the following: SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies); Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies); Comcast Cable Communications Management, LLC; CSC Holdings, LLC (solely with respect to its cable systems operating in New York, New Jersey, and Connecticut) (the Cablevision systems); and Time Warner Cable Inc.

Attachment B – Participating Content Owners Group

The members of the Participating Content Owners Group are the following:

1. MPAA and the following MPAA members: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc., and their successors and assigns.

2. RIAA and the following RIAA members: UMG Recordings, Inc., Warner Music Group, Sony Music Entertainment, and EMI Music North America, and their successors and assigns.

Attachment C – Independent Review Program

The Independent Review Program described below is intended to provide an alternative, fast, efficient and low-cost means for Subscribers and Copyright Owners to obtain independent resolution of genuine disputes that may occur in connection with the Copyright Alert program outlined in the Agreement. Its purpose is to provide a Subscriber with a non-exclusive procedure to seek review of Copyright Alerts associated with the Subscriber's account in the event a Mitigation Measure is about to be applied on the Subscriber's account.

The Independent Review process shall be just one avenue of appeal for Subscribers challenging such measure. This Independent Review process does not prevent Subscribers or Copyright Owners from addressing disputes through the courts, and that is the proper forum for addressing issues that are beyond the scope of this Independent Review process.

1. Grounds for Independent Review. Once a Subscriber has received a Copyright Alert stating that a Mitigation Measure is about to be applied, the Subscriber may request an Independent Review of that Copyright Alert and prior Copyright Alerts (as described in paragraph 4.1.4) on the following grounds:

(i) Misidentification of Account – that the ISP account has been incorrectly identified as one through which acts of alleged copyright infringement have occurred.

(ii) Unauthorized Use of Account – that the alleged activity was the result of the unauthorized use of the Subscriber's account of which the Subscriber was unaware and that the Subscriber could not reasonably have prevented.

(iii) Authorization – that the use of the work made by the Subscriber was authorized by its Copyright Owner.

(iv) Fair Use – that the Subscriber's reproducing the copyrighted work(s) and distributing it/them over a P2P network is defensible as a fair use.

(vi) Misidentification of File – that the file in question does not consist primarily of the alleged copyrighted work at issue.

(vii) Work Published Before 1923 – that the alleged copyrighted work was published prior to 1923.

All determinations shall be made by an independent "Reviewer" as described below, and the determinations shall have the effect set forth herein.

2. Standard of Review.

2.1. Misidentification of Account. A Subscriber shall prevail on this defense if the Participating ISP's and/or Copyright Owner's records indicate, upon Independent Review, that a factual error was made in (1) identifying the IP address at which the alleged copyright infringement occurred and/or (2) correlating the identified IP address to the Subscriber's account. In reviewing the Participating ISP's or Copyright Owner's records, automated systems for capturing IP addresses or other information in accordance with Methodologies have a rebuttable presumption that they work in accordance with their specifications, unless the Independent Expert's review of any such Content Owner Representative Methodology resulted in a Finding of Inadequacy in which event such rebuttable presumption shall not apply to such Content Owner Representative Methodology.

2.2. Unauthorized Use of Account. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that the alleged activity was the result of unauthorized use of the Subscriber's account by someone who is not a member or invitee of the household (*e.g.*, via an unsecured wireless router or a hacked Internet connection) of which the Subscriber was unaware and that the Subscriber could not reasonably have prevented. The foregoing sentence notwithstanding, the Reviewer may in his or her discretion conclude that a Subscriber is entitled to prevail under this defense despite the Subscriber's failure to secure a wireless router if the Reviewer otherwise concludes that the Subscriber adequately and credibly demonstrates that the alleged activity was the result of unauthorized use of the Subscriber's account by someone who is not a member or invitee of the household of which the Subscriber was unaware. In determining whether this standard has been satisfied, the Reviewer shall consider the evidence in light of the educational messages previously provided by the Participating ISP. Except as set forth herein, this defense may be asserted by a Subscriber only one (1) time to give the Subscriber the opportunity to take steps to prevent future unauthorized use of the Subscriber's account. Any subsequent assertion of this defense by a Subscriber shall be denied as barred, unless the Subscriber can show by clear and convincing evidence that the unauthorized use occurred despite reasonable steps to secure the Internet account and that the breach of such security could not reasonably have been avoided.

2.3. Authorization. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates with written or other documented evidence that the Subscriber's alleged activity was actually specifically authorized by the Copyright Owner or its authorized representative. Such written or other documented evidence typically must include a true and unaltered copy of the agreement or communication asserted to grant the claimed authorization. Such evidence shall not be deemed adequate and credible if, among other things, (i) the evidence on its face does not support a claim of authorization, (ii) the evidence does not appear authentic, or (iii) a reasonable person in the Subscriber's position would not have concluded that the communication was in fact authorizing the specific use made of the work and that such authorization came from the actual Copyright Owner or by someone authorized to act on his/her behalf. The defense shall fail if the Copyright Owner has demonstrated: (x) that the specific use of the work made by the Subscriber was not in fact authorized by the Copyright Owner; (y) if the

alleged authorization did not come directly from the Copyright Owner, that the person purporting to grant authorization was not authorized to act on behalf of the Copyright Owner for purposes of authorizing the specific use made of the work by the Subscriber; or (z) that the documentary evidence submitted by the Subscriber likely is not authentic or has been altered in a material manner.

2.4. Fair Use. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates fair use of the copyrighted work under prevailing principles of copyright law (which shall be identified as described in section 6).

2.5. Misidentification of File. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that a factual error was made in identifying the file at issue as consisting primarily of the alleged copyrighted work. In making this determination, the Content Owner Representative Methodology used to identify the file shall have a rebuttable presumption that it works in accordance with its specifications, unless the Independent Expert's review of any such Content Owner Representative Methodology resulted in a Finding of Inadequacy in which event such rebuttable presumption shall not apply to such Content Owner Representative Methodology.

2.6. Work Published Before 1923. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that the alleged copyrighted work in question was actually published prior to 1923.

3. Effect of Decision. If the Reviewer's decision is in favor of the Subscriber for a particular Copyright Alert, that Copyright Alert shall be deemed invalid, the filing fee described in paragraph 4.1.6 shall be promptly refunded to the Subscriber, and the Participating ISP shall remove that Copyright Alert from the Subscriber's account records and refrain from applying any Mitigation Measures based on the invalidated Copyright Alert(s). All other Copyright Alerts shall remain valid, and shall count toward future Mitigation Measures. If the Reviewer's decision for a particular Copyright Alert is in favor of the Copyright Owner, that Copyright Alert shall be deemed valid, and if applicable, the Mitigation Measure shall be applied promptly. The Reviewer's decision will be binding solely for the purposes of the Copyright Alert program. By participating in the Independent Review, the Subscriber, the Participating ISP, and the Copyright Owner agree to waive all rights to challenge the Reviewer's decision for purposes of the Copyright Alert program. The Reviewer's decision shall have no effect outside of the Copyright Alert program, shall not act as res judicata or collateral estoppel or any similar bar, and shall not have any precedential impact for other Independent Reviews with respect to other Subscribers within the Copyright Alert program. In any judicial proceeding between a Subscriber and a Copyright Owner concerning subject matter that is or has been the subject of Independent Review, neither the Subscriber nor the Copyright Owner shall seek to enter into evidence, or otherwise refer to or cite, either the fact of the Independent Review or any outcome of the Independent Review.

4. Independent Review Procedure.

4.1. How to Initiate an Independent Review.

4.1.1. *ACIR Form.* When the Participating ISP sends a Copyright Alert stating that the Subscriber's account is subject to a Mitigation Measure, the Participating ISP will also make available to the Subscriber access to an online Application to Commence Independent Review ("ACIR") form and related materials. The ACIR form and related materials will permit the Subscriber to review all of the Copyright Alerts applicable to the Subscriber's account that have not previously been subject to review, as further described in paragraph 4.1.4. The ACIR form will identify all of the information necessary for the Subscriber to invoke an Independent Review, including each defense asserted as to each work identified in a Copyright Alert under review, and also include space for provision of the Subscriber's contact information.

4.1.2. *Authorization.* The ACIR form will contain an authorization by the Subscriber to disclose relevant personal information to the Reviewer and to the Participating ISP. Such information includes: (1) information contained on the ACIR form, (2) information in the Participating ISP's possession, custody or control identifying the Subscriber or relating to any Copyright Alert sent to the Subscriber by the Participating ISP concerning alleged infringement, (3) information regarding the Participating ISP's matching of the IP address in an ISP Notice to the Subscriber's account, and (4) details of actions taken or proposed to be taken as Mitigation Measures by the Participating ISP with respect to the Subscriber's account. Except as explained in the next sentence or as required by judicial order or other legal process, all Subscriber personal information will be held in confidence and not disclosed to the Copyright Owner. If the Subscriber's defense is based on authorization, then the Reviewer may, in his or her discretion, disclose to the Copyright Owner only such personal information concerning the Subscriber as is reasonably necessary to permit the Copyright Owner to rebut a claim of authorization if that information is required for such purposes. The ACIR form will contain an authorization by the Subscriber to disclose relevant personal information to the Copyright Owner in the circumstances described in the immediately preceding sentence.

4.1.3. *Information Required.* The Subscriber must (1) identify the defenses asserted as to each work identified in each Copyright Alert at issue by checking the proper boxes on the ACIR form, (2) explain the specific basis for each defense, and (3) provide the corresponding back-up material to support such grounds. In the case of a defense of authorization, the ACIR form must be accompanied by the applicable written or other documented evidence that the Subscriber's alleged activity was specifically authorized by the Copyright Owner or its authorized representative, as described in paragraph 2.3. In the case of a defense of fair use, the ACIR form must (1) be accompanied by a true and unaltered copy of each content file that the Subscriber asserts to be a fair use under prevailing principles of copyright law; and (2) an explanation of each use

the Subscriber made of the file, including any distribution or downloading identified in the Copyright Alert(s), and the basis for claiming each such use as a fair use.

4.1.4. *Copyright Alerts Subject to Review*. The Subscriber shall have the right to invoke Independent Review for the last Copyright Alert sent as well as prior Copyright Alerts, provided that the right to have a particular Copyright Alert reviewed shall be waived if that right is not invoked the first time the Copyright Alert becomes eligible to be reviewed. Accordingly, when a Subscriber first receives a Mitigation Measure Copyright Alert, the Subscriber may invoke the Independent Review process as to any prior Copyright Alert, but if any of those Copyright Alerts is not reviewed at that time it will thereafter be unreviewable.

4.1.5. *Multiple Works Identified in a Copyright Alert*. In cases in which a Copyright Alert alleges infringing activity with respect to multiple works, the Independent Review process may be invoked by a Subscriber only if the Subscriber offers a defense as to every work cited in the Copyright Alert. A Copyright Alert will be considered valid and provide a basis for the application of a Mitigation Measure if the Subscriber is found to have no valid defense as to any one work cited in the Copyright Alert, unless the Independent Review establishes a pattern of invalid allegations in the Copyright Alert sufficient to cast substantial doubt on the Copyright Alert's remaining allegations.

4.1.6. *Filing Fee*. The Subscriber shall be required to pay a filing fee of thirty-five dollars ($35) in order to invoke the Independent Review, unless the Subscriber qualifies for a waiver or reduction in the filing fee in accordance with the procedures of the Administering Organization (as defined in paragraph 5.1 below). This fee will be refunded to the Subscriber in the event that the Reviewer decides in favor of the Subscriber as to any Copyright Alert eligible for review.

4.1.7. *Deadline*. The ACIR form, related materials and filing fee ("ACIR Package") must be submitted electronically within ten (10) business days after receipt of the relevant Copyright Alert. Except as contemplated in paragraph 5.6 below, failure to properly submit an ACIR form by the due date shall be deemed a waiver of the right to seek Independent Review regarding the applicable Mitigation Measure.

4.1.8. *Submission of ACIR Package*. The Subscriber must submit the ACIR Package to the Administering Organization. The Administering Organization shall immediately send a copy of the ACIR Package to the applicable Participating ISP.

4.1.9. *Effect of Filing for Independent Review*. A Subscriber's filing of the ACIR form stays implementation of any Mitigation Measure. A Subscriber's failure to file an ACIR or otherwise challenge an allegation of copyright

infringement shall not be construed as an admission or waiver in any other forum or context.

4.2 Process for Independent Review.

4.2.1. *Selection of Reviewer.* All Independent Reviews shall be resolved by one (1) individual serving as an independent Reviewer. The Reviewer will be selected by the Administering Organization from a panel of neutrals, as further described in paragraph 5.2.

4.2.2. *Initial Review of ACIR Package.* A Reviewer will review the ACIR package within five (5) business days of receipt to determine whether it is substantially complete. To be considered substantially complete, (1) the ACIR Package must include a substantially completed ACIR form; (2) the ACIR form must assert a defense as to each work identified in the relevant Copyright Alert subject to Independent Review; (3) for each defense asserted as to each work, the ACIR Package must include sufficient information as described in paragraph 4.1.3 to permit the Independent Review to proceed meaningfully and to potentially result in a decision in favor of the Subscriber; and (4) the ACIR Package must include the required payment as provided in paragraph 4.1.6. If the ACIR Package is not substantially complete, the case will be denied. The first time an ACIR Package is denied, such a denial shall be without prejudice to afford the Subscriber one additional opportunity to correct any mistakes or omissions in the ACIR Package. In such a case, the Reviewer shall notify the Subscriber of the relevant defects and afford the Subscriber five (5) business days to remedy the defects by submitting a substantially complete ACIR Package. Otherwise (except as provided in paragraph 5.6 below), such a denial shall be with prejudice. Either a denial without prejudice that is not remedied within 5 business days or a denial with prejudice shall have the same effects as a denial on the merits (see section 3).

4.2.3. *Verification that Defense of Unauthorized Use of Account is not Barred.* In the case of any defense of unauthorized use of account, the Reviewer's initial review will also consider whether that defense is barred because the Administering Organization's records indicate that the Subscriber previously asserted that defense in another Independent Review. If so, the defense shall be denied, unless the Subscriber can show by clear and convincing evidence that the unauthorized use occurred despite reasonable steps to secure the Internet account and that the breach of such security could not reasonably have been avoided. If for any reason the Administering Organization's records are inconclusive as to this question, the Reviewer will request clarification from the Participating ISP pursuant to paragraph 4.2.4.

4.2.4. *Collection of Standard Information from Participating ISP and Copyright Owner.* If the ACIR Package is substantially complete, the Reviewer will, if needed, request standard relevant information from the Participating ISP

and/or Copyright Owner to assess the grounds for review. Details of the standard information to be provided by the Participating ISP and/or Copyright Owner for different types of defenses shall be determined by mutual agreement of representatives of the Administering Organization, Participating ISPs and Copyright Owners as implementation proceeds, with the goal of having provision of this standard information be a straightforward and largely automated process. In the case of a defense of misidentification of account, information to be provided by the Participating ISP is anticipated to consist of information in the Participating ISP's possession, custody, or control relating to (1) ISP Notices received by the Participating ISP and matched to the Subscriber's account, (2) Copyright Alerts sent to the Subscriber by the Participating ISP, and (3) the Participating ISP's matching of IP addresses on ISP Notices received by the Participating ISP to the Subscriber's account. Information to be provided by the Copyright Owner is anticipated to consist of all or part of the evidence package(s) (*i.e.*, information relating to the alleged access to copyrighted material) for one (1) or more Copyright Alerts that are the subject of the Independent Review. The Participating ISP and Copyright Owner, as applicable, will provide the relevant information to the Reviewer within ten (10) business days after receipt of the request.

4.2.5. *First Substantive Review.* Within five (5) business days from receipt of the relevant standard information from the Participating ISP and/or the Copyright Owner, the Reviewer will review the case record substantively to determine if additional information from the Participating ISP and/or Copyright Owner is required, or whether it is apparent without soliciting further information that the Subscriber will not prevail as to all works cited in any one (1) or more Copyright Alerts.

4.2.6. *Supplemental Information.* The Reviewer shall have the discretion to request supplemental information from the Participating ISP, Copyright Owner or Subscriber within the five (5) business day period referred to in paragraph 4.2.5, if such information would likely be material to a just resolution of the Independent Review. If the Reviewer makes such a request, the applicable party(ies) shall have ten (10) business days to respond. If the Subscriber asserts a defense of authorization or fair use and the Reviewer determines that the defense may have merit, then the Copyright Owner shall receive all relevant information about the defense from the Reviewer and be afforded an opportunity to provide evidence to rebut the defense within ten (10) business days from receipt of such information. Such information shall include (1) in the case of a defense of authorization, all substantiating evidence and explanation submitted by the Subscriber as to each relevant work and the Subscriber's identifying information, unless the Reviewer concludes that the Copyright Owner does not need to know the identity of the Subscriber to evaluate the Subscriber's claim that his or her activity was authorized; and (2) in the case of a defense of fair use, the content file submitted by the Subscriber as to each relevant work and an explanation of why the Subscriber believes each use of that content file to be a fair use.

4.2.7. *Final Assessment and Issuance of Decision.* Within ten (10) business days of receipt of all requested information, including any supplemental information provided pursuant to paragraph 4.2.6, or passage of the relevant time to provide supplemental information in the event no supplemental information is received, the Reviewer shall assess the complete case record and enter a final decision. In doing so, the Reviewer shall determine the relevance, materiality and weight of all evidence based on the available record. The proceedings will take place exclusively on the written record, and there shall be no live hearings. For a Copyright Alert alleging infringement of multiple copyrighted works, in order to find in favor of the Subscriber with respect to the Copyright Alert, the Reviewer must consider and find in favor of the Subscriber as to a defense for each individual work referenced in the Copyright Alert or must find a pattern of invalid allegations in the Copyright Alert sufficient to cast substantial doubt on all allegations in the Copyright Alert. Upon reaching a final decision, the Reviewer will notify the Subscriber, Participating ISP and Copyright Owner of the outcome, and if the decision is a denial of the Subscriber's defense, the Reviewer will also include a short description of the rationale for the denial.

4.2.8. *Withdrawal of Notice by Copyright Owner.* A Copyright Owner may withdraw an ISP Notice at any time during the Independent Review process, which shall have the same effect as a finding for the Subscriber as to the withdrawn Copyright Alert (see section 3).

4.2.9. *Communications Among Parties.* Except as specifically described in these rules (*e.g.*, in the case of requests for information as described in paragraphs 4.2.4 and 4.2.6), there will be no communication between the Reviewer and the Participating ISP, Copyright Owner or Subscriber concerning the Independent Review. There is to be absolutely no discovery between the parties to the dispute, and no party shall have any obligation to respond to any request for information or to provide any particular information, except as described herein.

5. Administration of Independent Review Process.

5.1. In General. The Independent Review process shall be coordinated by the administering organization selected by the CCI Executive Committee ("Administering Organization"). The Independent Review process shall be governed exclusively by these rules.

5.2. Selection of Reviewers. The Administering Organization shall have mechanisms for establishing a panel of neutrals and for ensuring their continuing neutrality, their compliance with these rules, and their adherence to the governing principles of copyright law as provided in section 6. Reviewers must be lawyers, but need not necessarily have the legal or case management expertise that would qualify them to act as arbitrators of more complex disputes in a broader-ranging alternative

dispute resolution process. The Administering Organization shall provide Reviewers training in this Independent Review process and governing principles of copyright law determined as described in section 6. Reviewers may be staff employees of the Administering Organization if the volume of disputes subject to the Independent Review process so warrants.

5.3. Automation. The Administering Organization shall implement automated processes for managing the workflow of cases proceeding through the Independent Review process, including means for seeking and obtaining information from Participating ISPs and Copyright Owners in a manner that minimizes the associated workload on Participating ISPs and Copyright Owners and is automated to the maximum extent practicable.

5.4. Records of Subscriber History of Invoking Independent Review. The Administering Organization will maintain a secure database of Subscribers' history of invoking the Independent Review process, which will be available to Reviewers when evaluating future disputes involving the relevant Subscribers. Thus, for example, it should be possible for a Reviewer to determine from this database whether a Subscriber has previously asserted a defense of unauthorized use of account, and a Reviewer may consider a Subscriber's Independent Review history in evaluating the credibility of claims under review.

5.5. Recordkeeping and Review. The CCI Executive Committee and Administering Organization will establish processes for (1) maintaining records concerning proceedings, (2) periodically reviewing anonymous, aggregated information about issues and outcomes so that trends can be identified and addressed if warranted, and (3) confidentially auditing decisions for purposes of evaluating the performance of Reviewers and the Administering Organization. Except to the extent necessary to maintain records of outcomes of proceedings for purposes of operation and review of the Independent Review process or as otherwise expressly set forth herein, Reviewers shall not prepare written decisions in the cases they decide. The Parties to the Agreement agree to negotiate in good faith as to adjustments in the Independent Review process if such adjustments are warranted by actual experience in operating the Independent Review process.

5.6. Provision of Information. Fair and efficient administration of the Independent Review process depends upon timely provision of information requested by the Reviewer at various steps of the process, as described in paragraph 4.2. Whenever these rules set forth a timeframe for provision of information requested by the Reviewer, the Reviewer may grant reasonable extensions of such period (not to exceed ten (10) business days) for substantial good cause shown. In the absence of the requested information at the deadline for providing the same, the following provisions will apply:

5.6.1. *Delays in Providing Standard Information.* If the Reviewer properly requests a standard package of information from a Participating ISP or Copyright Owner, as described in paragraph 4.2.4, and the Participating ISP or

Copyright Owner does not provide the requested information as to some or all claims or works on a timely basis, (1) the Reviewer shall promptly notify the Participating ISP or Copyright Owner and the Participating ISP or Copyright Owner shall have a further five (5) business days to provide the requested information; and (2) the Administering Organization shall reflect such deficiency in reports to be provided periodically to the CCI Executive Committee. Recurring failure of a Participating ISP or Copyright Owner to provide requested standard information during the initial period identified in paragraph 4.2.4, in other than isolated instances, will be considered a breach of its obligations under the Agreement. If a Participating ISP or Copyright Owner does not provide available requested information within a further five (5) business days, (a) the dispute will proceed to the next step of decision making based on the available record without such information, giving the Subscriber the benefit of any doubt concerning the missing requested information; (b) the Administering Organization shall reflect such deficiency in reports to be provided periodically to the CCI Executive Committee; and (c) the Participating ISP or Copyright Owner will be considered in breach of its obligations under the Agreement.

5.6.2. *Delays in Providing Supplemental Information.* If the Reviewer properly requests supplemental information from a Participating ISP, Copyright Owner or Subscriber pursuant to paragraph 4.2.6, and the Participating ISP, Copyright Owner or Subscriber does not provide the requested information as to some or all claims or works on a timely basis, the dispute will proceed to the next step of decision making based on the available record without such information. If the Reviewer believes that the position of a party to the proceeding other than the one that has failed to provide the requested information is otherwise meritorious, the Reviewer shall give such party the benefit of any doubt concerning the missing requested information.

6. Legal Principles to Be Applied in Independent Review. The Independent Review process will, to the extent relevant, apply prevailing legal principles as determined by United States federal courts. The Administering Organization will commission an accepted, independent expert on copyright law, who is approved by the CCI Executive Committee, to outline prevailing legal principles of fair use for purposes of deciding defenses of fair use, and any other legal principles necessary for resolution of issues within the scope of this Independent Review process. Such outline will be updated from time to time as necessary. If additional material questions of law arise as the Independent Review process is implemented, they may be referred to an accepted, independent expert approved by the CCI Executive Committee as needed. The Administering Organization will advise the Parties to the Agreement of issues referred to, and principles determined by, such an expert, and provide a process for the Parties to the Agreement to provide input concerning the issues, so as to ensure that the expert's determinations are fully-informed and reflect prevailing law as determined by United States federal courts.

Attachment D – MPAA Member Company Affiliates

The MPAA member companies' affiliates are entities under the control of an MPAA member company. For purposes of this Attachment D, "control" is defined as (1) the ownership of at least fifty percent (50%) of the equity or beneficial interest of the controlled entity, (2) the right to vote for or appoint a majority of the board of directors or other governing body of such entity (if the board or governing body may exercise authority with less than a majority, then the right to vote or appoint the number of directors necessary to exercise that authority), or (3) the right or authority to grant, approve or withhold, directly or indirectly, financial resources necessary to the operation of the controlled entity. As of the Effective Date of this Agreement, the following entities are MPAA member company affiliates:

- Disney Enterprises, Inc., entities controlled, directly or indirectly, by Disney Enterprises, Inc. (together, "Disney Enterprises Entities"), and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by Disney Enterprises Entities.
- Fox Entertainment Group, Inc., entities controlled, directly or indirectly, by Fox Entertainment Group, Inc., (together, "Fox Entertainment Entities") and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by Fox Entertainment Entities.
- NBCUniversal Media LLC, entities controlled, directly or indirectly, by NBCUniversal Media LLC, (together, "NBCU Entities") and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by NBCU Entities.
- Sony Pictures Entertainment Inc., entities controlled, directly or indirectly, by Sony Pictures Entertainment Inc. (together, "SPE Entities"), and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by SPE Entities.
- Turner Entertainment Networks, Inc., entities controlled, directly or indirectly, by Turner Entertainment Networks, Inc. (together, "Turner Entities"), and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by Turner Entities.
- Viacom, Inc., entities controlled, directly or indirectly, by Viacom, Inc. (together, "Viacom Entities"), and such other entities as have authorized the foregoing to send notices on their behalf with respect to works distributed by Viacom Entities.
- Walt Disney Studios Motion Pictures, entities controlled, directly or indirectly, by Walt Disney Studios Motion Pictures (together, "Walt Disney Studios Entities"), and such other entities as have authorized the foregoing to send notices on their behalf with respect to works distributed by Walt Disney Studios Entities.
- Warner Bros. Entertainment Inc., entities controlled, directly or indirectly, by Warner Bros. Entertainment Inc. (together, "Warner Bros. Entities"), and such other entities as have authorized the foregoing to send notices on their behalf with respect to works distributed by Warner Bros. Entities.

Graduated Response American Style: "Six Strikes" Measured Against Five Norms

Annemarie Bridy*

Read 10/25 flight

Table of Contents

Introduction 3
I. The Graduated Response Paradigm 5
A. Graduated Response Generally 6
B. The Domestic Roots of Graduated Response 6
C. The Global Campaign for Graduated Response 8
II. In the EU: Two Takes on "Three Strikes" 12
A. Graduated Response as Public Law: The French Example (Hadopi) 12
B. Graduated Response as Private Law: The Irish Example (Eircom) 16
III. In the US: Six Strikes (But You're Probably Not Out) 18
A. The Center for Copyright Information (CCI) 18
B. The Copyright Alert System (CAS) 20
1. The Six Strikes Protocol 20
2. The Appeal Process 22
IV. Five Norms for Measuring Six Strikes 24
A. Freedom of Expression 25
1. Suspension of Access 25
2. Content Filtering 26
B. Privacy 28
1. Surveillance 28
2. Loss of Anonymity 32
C. Fairness 33

* Associate Professor of Law, University of Idaho College of Law. This article was initially presented at "Copyright Cat and Mouse: New Developments in Online Enforcement," a multi-stakeholder symposium on the "Six Strikes" MOU sponsored by the Princeton University Center for Information Technology Policy (CITP). I would like to thank CITP, Ed Felten, and Steve Schultze for their invitation to participate in that symposium and for their support during my semester in residence at Princeton during Spring 2012. I would also like to thank the participants in the Second Annual Internet Law Scholars Works in Progress (ILSWIP) Conference at New York Law School and the Twelfth Annual Intellectual Property Scholars Conference (IPSC) at Stanford Law School, who provided valuable feedback as the article took shape. Finally, I owe special thanks to Monica Horten, Mary LaFrance, and Peter Yu, who provided very helpful comments on the complete draft.

1. Presumption of Innocence 33
2. Opportunity for Neutral Adjudication 34
3. Predictable Application of Established Legal Standards 35
4. Availability of Defenses 37
D. Proportionality 38
1. Necessity 38
2. Suitability 39
3. Burden on Individual Rights 39
E. Transparency 39
1. Design 40
2. Implementation 40
3. Outcomes 41
Conclusion 42

Introduction

From the earliest days of the commercial Internet, corporate copyright owners have been trying to get Internet service providers (ISPs) to play a more active role in the seemingly Sisyphean task of online copyright enforcement. Indeed, Congress recognized in 1998, when it passed the Digital Millennium Copyright Act (DMCA), that active cooperation between the two sets of stakeholders would be necessary to ensure effective enforcement of copyrights in the digital environment.[1] The DMCA, accordingly, sought to balance the burdens and interests of copyright owners and ISPs by establishing a fairly clear division of labor: copyright owners are charged with monitoring networks and services for infringing content, and ISPs are charged with promptly removing that content when they become aware of it and are situated to remove or disable access to it.[2] While the DMCA's statutory division of labor has worked relatively well over the years to manage large scale infringement on services that store content for users, it has not worked well to manage infringement over peer-to-peer (P2P) file sharing networks.[3] This is due in large part to a basic mismatch between the decentralized network architecture of P2P systems and the DMCA's assumption of a more centralized architecture in which ISPs host content uploaded by users.[4]

In 2008, in recognition of the DMCA's inadequacy in the face of P2P file sharing, and with the high-profile case of *Arista Records v. Lime Group*[5] pending in federal district court in New York, then New York State Attorney General Andrew Cuomo began pressuring broadband providers to agree voluntarily to play a greater role in fighting online infringement.[6]

---

[1] *See* H.R. Rep. No. 105-796, at 71 (1998) ("Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."); S. Rep. No. 105-190, at 19 (1998) (same).

[2] *See* 17 U.S.C. § 512 (c) (setting forth the DMCA's notice-and-takedown framework); 17 U.S.C. § 512(m) (providing that ISPs are not required to monitor their services for infringement). ISPs are also tasked under the DMCA with identifying alleged infringers to copyright owners who subpoena their identities and with implementing a program to terminate the accounts of repeat infringers. *See* 17 U.S.C.§ 512(h) (setting forth a framework for copyright owners to obtain pre-litigation subpoenas to identify alleged infringers); 17 U.S.C. § 512(i) (requiring ISPs to adopt and reasonably implement a program for terminating the access or accounts of repeat infringers).

[3] I have described this problem elsewhere at length as the DMCA's failure to scale for P2P infringements. *See* Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695 (2011). *See also* Jerome H. Reichman, Graeme B. Dinwoodie, & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 994 (2007) (concluding, with respect to storage providers, that "the past decade of experience with the DMCA notice and takedown regime suggests that a relatively balanced and workable solution to this particular dual-use technology problem has been found").

[4] Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 113 (2007) (remarking on the obsolescence of the DMCA's safe harbors in light of P2P technology); Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 41 (2006) ("[The DMCA] was designed to address a mainly centralized architecture . . . . Peer-to-peer architecture, by contrast, is decentralized and allows users to search for files stored in the libraries of other users.").

[5] In the case, Arista Records and a dozen music industry co-plaintiffs sued the operators of the LimeWire P2P service for secondary copyright infringement. *See* Arista Records LLC v. Lime Group LLC, 532 F. Supp. 2d 556 (S.D.N.Y. 2007). The service would later be shut down by court order following a grant of summary judgment to the plaintiffs. *See* Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481 (S.D.N.Y. 2010).

[6] *See* Bernadette Tansey, *New Tactic Fights File Sharing*, SAN FRANCISCO CHRONICLE, December 20, 2008, C1 ("The [Recording Industry Association of America (RIAA)] said New York Attorney General Andrew

Subsequently, at the national and international levels, the Obama administration endorsed the concept of privately negotiated collaborations between corporate rights owners and broadband providers. On the national level, the White House Office of the Intellectual Property Enforcement Coordinator (IPEC) in successive annual strategic plans encouraged private sector partnerships to curb repeat infringement.[7] On the international level, the United States Trade Representative (USTR) negotiated—and the United States ultimately signed—the controversial Anti-Counterfeiting Trade Agreement (ACTA), which contains a provision requiring parties to promote such partnerships.[8] In addition, the Organization for Economic Cooperation and Development (OECD), of which the United States is a member, promulgated a set of principles for Internet policy making in 2011 that encourages member countries to "foster voluntarily developed codes of conduct" within the private sector to curb illegal behaviors online.[9]

In July of 2011, broadband providers finally bowed to the mounting political pressure[10] and to changing economic realities in the business of corporate content ownership and delivery.[11] Five of the largest telecommunications companies in the United States entered into a memorandum of understanding (MOU) with trade groups representing major corporate copyright owners.[12] The MOU creates what the parties characterize as "a common framework of 'best

---

Cuomo is helping the industry develop an alternative to its mass courtroom campaign by promoting its talks with Internet providers.").

[7] OFFICE OF THE INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 17 (2010) (stating that "[t]he Administration believes that it is essential for the private sector…to work collaboratively…to seek practical and efficient solutions to address infringement"); 2011 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 5 (2011) (stating that "[t]he Administration is committed to facilitating practical and efficient voluntary actions by the private sector").

[8] Anti-Counterfeiting Trade Agreement art. 27, Oct. 1, 2011,*available at* http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf. The parties to ACTA are Australia, Canada, the European Union and its member states, Japan, Korea, Mexico, Morocco, New Zealand, Singapore, Switzerland and the United States.

[9] *See* ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY MAKING 7 (2011) ("These codes would be developed by voluntary participants in a multi-stakeholder process...[and] should encourage and facilitate voluntary co-operative efforts by the private sector to…address illegal activity…taking place over the Internet.").

[10] As Derek Bambauer has pointed out, the nature and extent of the government's role in brokering the deal are difficult to pin down. *See* Bambauer, *supra* note ___, at ____. Governor Cuomo's role was sufficiently substantial, however, to elicit a public expression of thanks from the parties to the MOU for his "deep involvement and personal efforts" in bringing the deal to fruition. *See* Press Release, Center for Copyright Information, Music, Movie, TV and Broadband Leaders Team to Curb Online Content Theft: Announce Common Framework for "Copyright Alerts" (July 7, 2011), http://www.copyrightinformation.org/node/704.

[11] *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81 (2010); Annemarie Bridy, *ACTA and the Specter of Graduated Response*, 26 AM. U. INT'L L. REV. 558 (2011). The 2011 merger between Comcast, traditionally a conduit for content, and NBC Universal, traditionally an owner of rights in content, is a prime example of the substantial realignment of interests that has occurred between broadband providers and corporate copyright owners in the dozen or so years since the DMCA became law. *See* Bridy, *ACTA and the Specter of Graduated Response*, at 571-72 (discussing the rise of streaming-over-broadband and the blurring lines of demarcation between corporate content producers and corporate network operators). At the 2010 State of the Net Conference, Comcast CEO Brian Roberts acknowledged a significant merger-induced shift in Comcast's corporate perspective on online copyright enforcement: "The whole question of piracy, we are now going to be on both sides of that issue." Kenneth Corbin, *Comcast Set to Enter Copyright Wars*, DATAMATION.COM, Jan. 27, 2010 (quoting Roberts).

[12] *See* Memorandum of Understanding (hereinafter "MOU"), July 6, 2011, http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf . The

practices' to effectively alert subscribers, protect copyrighted content and promote access to legal online content."[13] At the core of the common framework is the Copyright Alert System (CAS), a domestic graduated response system that differs in significant respects from the controversial "three strikes" model currently operating in several countries abroad, most notably in France.[14] CAS is a privately designed and administered enforcement system to which members of the public opt in through contractual terms of service with their broadband providers.[15] It applies only to users of residential broadband services and is intended to address infringement only over P2P networks.

This Article is an assessment of CAS with respect to five norms that are central to consumer protection in the enterprise of online copyright enforcement: freedom of expression, privacy, fairness, proportionality, and transparency. Part I provides an introduction to graduated response, which is the genus of online copyright enforcement to which CAS belongs. Part II takes a comparative look at two pre-existing graduated response systems: the government mandated and administered program in France, Hadopi, and a privately administered program in Ireland run by the broadband provider Eircom. Part III provides a detailed explanation of CAS, including its governance structure, the division of labor it prescribes between copyright owners and broadband providers, and the graduated system of warnings and sanctions that it employs. Part IV evaluates the strengths and weaknesses of CAS with respect to each of the five norms listed above, using the systems in France and Ireland as reference points.[16]

I. The Graduated Response Paradigm

This Part begins with a general discussion of graduated response as an online copyright enforcement mechanism and then goes on to consider its origins in U.S. copyright policy and its rise to prominence on the global enforcement agenda of corporate rights owners.

---

participating ISPs are AT&T, Verizon, Comcast, CSC Holdings (Cablevision), and Time Warner. *Id.* at 24 (Attachment A). The participating corporate rights owners are members of the Motion Picture Association of America (MPAA) (Disney, Paramount, Sony, Twentieth Century Fox, Universal, and Warner Bros.) and the RIAA (UMG, Warner, Sony, and EMI). *Id.* at 25 (Attachment B). Groups representing independent filmmakers and artists—the American Association of Independent Music (A2IM) and the Independent Film and Television Alliance (IFTA)—are also included. *Id.* at 2.

[13] Center for Copyright Information, Press Release, Music, Movie, TV and Broadband Leaders Team to Curb Online Content Theft: Announce Common Framework for "Copyright Alerts, July, 7, 2011, http://www.copyrightinformation.org/node/704.

[14] *See* MOU, *supra* note 12, at 1 (introducing the idea of "[a] reasonable alert-based approach") and 7-14 (setting forth the technical requirements of CAS). The French system will be discussed in Part I.B. *infra*.

[15] *See id.* at 7 (requiring party ISPs to amend their terms of service or acceptable use policies to incorporate CAS).

[16] I have omitted competition from the list, although it is a decidedly important consumer value, because any detailed discussion of the antitrust implications of the formation of CCI and the operation of CAS must lie beyond the scope of this project. Questions about the legality of CCI and CAS under antitrust law are very much alive and are currently being explored by others. *See* Timothy B. Lee, *What the 1930s Fashion Industry Tells Us About Big Content's "Six Strikes" Plan*, ARS TECHNICA, July, 28, 2011 (quoting Mark Patterson of Fordham Law School).

A. Graduated Response Generally

Graduated response is a copyright enforcement paradigm designed to address the phenomenon of repeat infringement over digital networks. In general, graduated response involves a series of notifications and warnings that culminate in the imposition of a sanction or sanctions intended to deter future infringements.[17] The most common form of graduated response is the "three strikes and you're out" model, in which a user's Internet access is suspended by his or her ISP following the receipt of three successive notices of copyright infringement over a set period of time.[18] Shared enforcement between rights owners and ISPs is the hallmark of graduated response, although the precise division of labor between the two sides with respect to traffic monitoring and user notification can vary from one implementation to the next.[19]

B. The Domestic Roots of Graduated Response

The domestic roots of graduated response can be traced back to the DMCA and its "repeat infringer" provision, which conditions an ISP's eligibility for safe harbor from claims of secondary copyright infringement on the ISP's adoption and implementation of a policy that provides for termination of access for repeat infringers.[20] Unlike the notice and takedown provision in the DMCA, which applies to services that store data for users (e.g., user-generated content sharing platforms like Flickr and YouTube) but not to service providers that simply route and transmit their users' data (e.g, broadband providers like AT&T, Verizon, and Comcast), the repeat infringer provision applies equally to all ISPs, including broadband providers.[21]

Oh I forgot about that section

One might expect broadband providers' compliance with the repeat infringer provision to result fairly routinely in account terminations for P2P users who engage in a high volume of illegal file sharing. In practice, however, that has not been the case. Reaching consensus on precisely what the DMCA requires of ISPs with respect to repeat infringement has been difficult for two reasons: first, the statute does not define what a repeat infringer is; second, courts have been deferential to service providers concerning the substance and form of their individual repeat

---

[17] *See, e.g.*, IFPI, 2011 Digital Music Report, at 18 (defining graduated response).

[18] *See generally* Peter Yu, *The Graduated Response*, 62 FL. L. REV. 1373 (2010).

[19] Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at 84. The most controversial protocol proposed by industry trade groups is an ISP-centric one that involves automated in-network monitoring and blocking of copyrighted files. Some U.S. colleges and universities have already adopted in-network filtering to comply with the Higher Education Act, which, since 2008, has conditioned participation in federal student aid programs on an institution's development of copyright enforcement plans that include technology-based deterrents to online infringement. *See* 20 U.S.C.S. § 1094(a)(29)(A) (LexisNexis 2009); 34 C.F.R. § 668.14 (2010).

[20] 17 U.S.C. § 512(i)(1)(A); Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004).

[21] Providers that perform routing and transmission services for users are covered by the safe harbor in section 512(a) of the DMCA, which governs transitory digital network communications. 17 U.S.C. § 512(a). These providers are not subject to the notice and takedown framework outlined in section 512(c). *In re* Charter Commc'ns, Inc., 393 F.3d 771, 776 (8th Cir. 2005) (noting that Section 512(a) does not require compliance with the DMCA's notice and takedown provisions). Providers that store information at the direction of users are covered by section 512(c) and are subject to the notice and takedown framework set forth in that section. 17 U.S.C. § 512(c). All providers seeking safe harbor under the DMCA are subject to section 512(i), which is the repeat infringer provision. Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 758 (9th Cir. 2007) (stating that "[t]o be eligible for any of the four safe harbors at §§ 512(a)–(d), a service provider must first meet the threshold conditions set out in § 512(i)").

agreement to let sleeping dogs lie when it comes to repeat infringers and the DMCA, the MOU was born.[28]

Based on public statements by industry representatives, the MOU was a little over three years in the making, with serious negotiations getting underway in the spring and summer of 2008.[29] In December of 2008, the RIAA prematurely went public with news of a deal, which prompted some pointed denials from the broadband industry.[30] It seems probable that some agreement in principle had been reached by that point, but the devil being in the details, broadband providers were not yet willing to commit publicly to the inter-industry partnership. Their reticence on the matter ended with the press release announcing the MOU in July of 2011.[31]

C. The Global Campaign for Graduated Response

The international campaign for graduated response was already in high gear by the time Andrew Cuomo brought U.S.-based ISPs to the table with corporate rights owners in 2008.[32] An official declaration released during the 2005 Cannes Film Festival by European Union (EU) culture and audiovisual ministers touted graduated response as "a major step forward" in the "exchange of best practices in the fight against piracy" and concluded that it would be "useful" for European governments "[t]o foster agreements between rights holders and access providers."[33] The meeting that produced the Cannes Declaration brought film and telecommunications industry executives together with European culture ministers under the auspices of the French Ministry for Culture and Communications and the EU Information Society Commissioner to discuss the future of online film distribution for European filmmakers.[34] In the European campaign to promote graduated response, the French took the lead in what then President Nicolas Sarkozy characterized as a crusade to "civilize" the Internet.[35] For his outspoken public support of graduated response legislation and, even more controversially,

---

[28] The parties to the MOU expressly provide that the agreement "does not and is not intended to create any obligation on a Participating ISP to…implement, enforce, or otherwise take any action in furtherance of a DMCA Termination Policy." MOU, *supra* note 12, at 9 n.1. Another provision affirms that no step undertaken by ISPs to comply with the terms of the MOU "alters, expands, or otherwise affects any Participating ISP's rights or obligations under the DMCA." MOU, *supra* note 12, at 7.

[29] Anderson, *supra* note 21 (quoting Cary Sherman, who stated that discussions with broadband providers about graduated response had been going on for about a year (i.e., since 2007), but had picked up during the spring and summer (i.e., of 2008)). According to the IFPI, negotiations lasted for two years. IFPI, 2012 Digital Music Report, at 21.

[30] *See* Chloe Albanesius, *Comcast, Others Deny 'Three Strikes' Piracy Plan*, PCMAG.COM (Mar. 27, 2009); David Kravets, *Top Internet Providers Cool to RIAA 3-Strikes Plan*,WIRED (Jan. 5, 2009).

[31] Center for Copyright Information, Press Release, Music, Movie, TV and Broadband Leaders Team to Curb Online Content Theft: Announce Common Framework for "Copyright Alerts, July, 7, 2011, http://www.copyrightinformation.org/node/704.

[32] *See* Tansey, *supra* note 6 (discussing Cuomo's intervention on behalf of the music and film industries).

[33] Declaration of the European Ministers for Audiovisual Affairs and the Member of the Commission in charge of Information Society and Media attending the 2005 Europe Day at Cannes, http://ec.europa.eu/avpolicy/docs/other_actions/cannes_decl_2005_en.pdf.

[34] Declaration of the European Ministers, *supra* note --. *See also* MONICA HORTEN, THE COPYRIGHT ENFORCEMENT ENIGMA: INTERNET POLITICS AND THE 'TELECOMS PACKAGE' 84 (2012).

[35] *See* Milton U. Müller, *Activists Fear Sarkozy's Efforts to Tame Web*, SPIEGEL ONLINE INT'L, May 24, 2011, http://www.spiegel.de/international/europe/0,1518,764305,00.html.

infringer policies.[22] While at least one broadband provider has reported terminating access under the DMCA for the small number of subscribers who fail to heed repeated warnings concerning illegal file sharing, others have taken the entirely defensible position that they will not terminate a subscriber's access under the DMCA absent a court order identifying the subscriber as a repeat infringer.[23] The upshot is that there is no statutory requirement for graduated response in the United States, although an ISP's adoption of a three strikes protocol or some variant thereof would be sufficient for DMCA compliance.[24] Without any clear direction from the statute itself or from courts interpreting it, broadband providers and copyright owners have lived for some time with irreconcilable differences over what it takes to comply. Given this impasse, ISPs have had little incentive to interpret the requirements for compliance in ways that might alienate subscribers or raise the cost of doing business.

In the United States, privately ordered graduated response has been the entertainment industries' preferred plan for dealing with P2P infringement since the Recording Industry Association of America (RIAA) ended its multi-year campaign of litigation against individual file sharers in 2008.[25] At that time, entertainment industry representatives and their counterparts in the broadband industry were lobbying energetically against net neutrality regulation that threatened to prevent ISPs from implementing technical measures—e.g., filtering and protocol-based throttling—to control network congestion caused in part by P2P file sharing.[26] With the increasing popularity of legal streaming services and Internet-enabled high-definition TVs, ISPs seeking to optimize bandwidth usage discovered a powerful new incentive to collaborate with copyright owners to curb illegal P2P traffic.[27] Out of this mutuality of interests, and an

---

[22] *See* Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at 91 (discussing why the repeat infringer provision has not led to large numbers of account terminations for repeat infringers).

[23] Cox Communications admitted publicly that it has terminated subscriber access in a very limited number of cases. Sarah McBride, *Relationship Status of RIAA and ISPs: It's Complicated*, WALL ST. J. BLOG (Mar. 26, 2009, 3:07 PM), http://blogs.wsj.com/digits/2009/03/26/relationship-status-of-riaa-and-isps-itscomplicated/. AT&T has said that it will not terminate a customer's service for repeat infringement without a court order. Greg Sandoval, *How Charter Communications Warns Accused File Sharers*, CNET, April 19, 2009, http://news.cnet.com/8301-1023_3-10222853-93.html.

[24] Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at ___.

[25] Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1 (reporting on the transition from litigation to graduated response); Nate Anderson, *RIAA Graduated Response Plan: Q&A with Cary Sherman*, ARS TECHNICA, Dec. 21, 2008 (interviewing the RIAA's Cary Sherman about graduated response).

[26] *See The Internet Freedom Preservation Act of 2008: Hearing on H.R. 5353 Before the H. Subcomm. on Telecomms. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. (2008) (written statement of Mitch Bainwol, Chairman and CEO, RIAA), *available at* http://76.74.24.142/F382DD78-ECE4-2026-BD0C-33C4ED1A0D44.pdf ("Our view is that the marketplace is generally a better mechanism than regulation for addressing such complex issues as how to address online piracy."); Grant Gross, *AT&T Accused of 'Astroturfing' on Net Neutrality*, PCWORLD, Oct. 20, 2009, https://www.pcworld.com/article/173988/atandt_accused_of_astroturfing_on_net_neutrality.html (reporting on AT&T's efforts to bolster opposition to proposed net neutrality regulations); Saul Hansell, *Hollywood Wants Internet Providers to Block Copyrighted Files*, N.Y. TIMES, Sept. 25, 2008, http://bits.blogs.nytimes.com/2008/09/25/hollywood-tries-to-get-support-for-having-isps-block-copyrighted-files/ (reporting on the formation of the inter-industry lobbying group Arts + Labs).

[27] *See* Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at __.

in-network filtering, Sarkozy earned praise from the International Federation of the Phonographic Industry (IFPI) as "an example to others."[36]

In 2006, the copyright industries welcomed the publication of a government-commissioned report in the United Kingdom (UK) recommending that ISPs voluntarily adopt a "Best Common Practice (BCP) document" for coordinating with rights owners "to remove and disbar users engaged in 'piracy.'"[37] The report also recommended that legislation mandating user disconnection be introduced if a voluntary agreement could not be achieved by the end of 2007.[38] As things played out, the British government pressed for and brokered an MOU in 2008 between copyright industry trade groups and ISPs in which the parties agreed to work toward a significant reduction in P2P file sharing.[39] That MOU expired in 2009, however, after a three-month trial period.[40] Following the expiration of the MOU, copyright owners continued to press for government intervention, and passage of the Digital Economy Act of 2010 (DEA) made inter-industry cooperation the law.[41] The DEA gives Ofcom, Britain's telecommunications regulator, responsibility for approving or making (if none is submitted for approval) an initial code of obligations for ISPs to follow.[42] The DEA contemplates at minimum a notice regime and gives the Secretary of State authority to phase in additional obligations for ISPs, including a mandate to disconnect repeat infringers, if a notice-only regime proves ineffective.[43] Through the DEA, the British government has established a co-regulatory framework within which regulators will monitor ISP compliance with an industry-developed, government-approved code of conduct and will impose additional obligations on ISPs if specified reductions in file sharing volumes are not timely achieved.[44] The English have thus taken a graduated approach to graduated response.[45]

The concerted push for legislative mandates in France and the UK unfolded within the broader context of the EU telecommunications framework review, which began in 2007 and concluded in 2009 with the European Parliament's approval of the Telecoms Package.[46] At the

---

[36] *See* Jacqui Cheng, *French Cabinet Backs "Educational" Three-Strikes Law*, ARS TECHNICA, June 20, 2008, http://arstechnica.com/tech-policy/news/2008/06/frances-three-strikes-copyright-law-gets-cabinet-support.ars.

[37] HM Treasury, The Gowers Review of Intellectual Property 103 (2006); Int'l Fed'n of the Phonographic Indus, Press Release, IFPI Welcomes Parliamentary Report on Intellectual Property, May 15, 2007, http://www.ifpi.org/content/section_news/20070516.html.

[38] *Id.*

[39] Andrew Orlowski, *Feargal Sharkey on the ISP Filesharer MoU*, THE REGISTER, July 24, 2008 (reporting that minister Baroness Vadera at the Department for Business, Enterprise & Regulatory Reform intervened to bring about the deal and that Ofcom agreed to act as an "honest broker" between ISPs and rights owners in the negotiation of the MOU).

[40] CHRISTOPHER T. MARSDEN, INTERNET CO-REGULATION 210 (2011).

[41] *Id.* at 211-14 (describing events leading to the passage of the DEA).

[42] Digital Economy Act, 2010, c. 24 §§ 5-6 (U.K.); Digital Economy Act, 2010, c. 24, Explanatory Notes, ¶ 32.

[43] Digital Economy Act, 2010, c. 24 §§ 3-18 (U.K.); Digital Economy Act, 2010, c. 24, Explanatory Notes, ¶ 33.

[44] *See* MARSDEN, *supra* note 40, at 54 (defining co-regulation as a middle ground between direct government regulation of industry and industry self-regulation).

[45] *See generally* Anne Barron, *'Graduated Response' à l'Anglaise: Online Copyright Infringement and the Digital Economy Act of 2010*, 3 J. MEDIA L. 305 (2011) (providing a very thorough discussion of the DEA).

[46] Monica Horten offers a painstaking, document-driven analysis of the EU telecom reform process and how it came to be dominated by debates over graduated response and ISP secondary liability for online copyright

outset, the copyright industries viewed the telecoms framework review process as an opportunity to push for a Europe-wide, top-down graduated response mandate.[47] The simple version of the highly fraught political narrative that ensued is that various provisions requiring ISPs to sanction users for copyright infringement were proposed and debated, but they were ultimately defeated due to concerns among members of the EU parliament about freedom of expression, privacy, and due process of law.[48] In the end, individual member states were left to decide whether to require ISPs to implement graduated response.[49] The final Telecoms Package did, however, incorporate language intended to insure that the individual rights and fundamental freedoms of Internet users will not be sacrificed to the interests of copyright owners in member states that do elect to implement mandatory graduated response regimes.[50]

In addition to lobbying in individual European capitals and the EU's *de facto* capital of Brussels, the copyright industries have lobbied aggressively for graduated response in the international trade policy arena, where their collective interests are represented by the International Intellectual Property Alliance (IIPA).[51] In addition to dispatching its representatives to testify before national legislatures considering adopting graduated response mandates,[52] the IIPA participates annually in the United States Trade Representative's Special 301 process for identifying foreign countries that may be candidates for trade sanctions for failing to protect and enforce American intellectual property rights.[53] The IIPA's annual Special 301 report typically takes a wide array of individual governments to task for failing to use their power to combat digital piracy by creating strong legal incentives for ISPs to cooperate with copyright owners.[54] Since 2009, the IIPA has used the Special 301 process to focus its members' disapproval on individual governments, including those of Sweden, Japan, Hong Kong, and Singapore, among others.[55]

---

infringement. *See* MONICA HORTEN, THE COPYRIGHT ENFORCEMENT ENIGMA: INTERNET POLITICS AND THE 'TELECOMS PACKAGE' (2012).

[47] *Id.* at 103.

[48] *See id.* at 122-25, 5. The amendment that was ultimately adopted "neither mandates nor prohibits" national graduated response regimes. Directive 2009/136/EC, art. 1, 2009 OJ (L337) 21.

[49] *Id.* at 213-14.

[50] Directive 2009/136/EC, art. 1, 2009 OJ (L337) 21 ("National measures regarding end-users' access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process, as defined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.").

[51] They are represented in this arena primarily by the International Intellectual Property Alliance (IIPA). Members of the IIPA include the RIAA and the MPAA in addition to the Business Software Alliance (BSA), the Association of American Publishers (AAP), the Entertainment Software Association (ESA), the Independent Film & Television Alliance (IFTA), and the National Music Publishers' Association (NMPA).

[52] New Zealand is a case in point. *See* Testimony of the International Intellectual Property Alliance Before the House of Representatives Select Committee on Commerce on the Copyright (Infringing File Sharing) Amendment Bill, June 16, 2010.

[53] *See generally* Int'l Intellectual Property Alliance (IIPA), Special 301, http://www.iipa.com/special301.html.

[54] *See* generally Int'l Intellectual Property Alliance, Special 301 Reports (2009-2012), http://www.iipa.com/special301.html (last visited March 1, 2012).

[55] *See id.*

The IIPA was successful—although not nearly as successful as it would have liked—at having language promoting graduated response incorporated into ACTA.[56] During ACTA's negotiations, there was concern among civil society groups and other observers that the agreement would contain a binding requirement for signatories to legislate graduated response into their domestic copyright regimes.[57] Although the final agreement does not contain a DMCA-style repeat infringer provision or a mandate for graduated response legislation, it does require signatories "to endeavor to promote cooperative relationships within the business community to effectively address [online copyright infringement]."[58] Such language implies graduated response to anyone familiar with the rhetoric crafted to sell the concept to policy makers.[59]

A mandatory repeat infringer provision may yet end up in the final text of the Trans-Pacific Partnership (TPP) Agreement, another multilateral trade agreement, for which negotiations began in 2009.[60] A leaked draft of the TPP contains a repeat infringer provision virtually identical to the one in the DMCA.[61] The same provision appeared in early drafts of ACTA.[62] The TPP negotiating process has thus given copyright owners a second bite at the apple when it comes to their global ambitions for graduated response. It remains to be seen whether their persistence will pay off.

It is clear, however, from the debates surrounding both ACTA and the EU Telecoms Package that the global push for graduated response has met with pushback. The governments of Germany and Spain rejected graduated response even as legislation requiring it advanced elsewhere within the EU.[63] Moreover, the United Nations (UN) General Assembly and the EU's Data Protection Supervisor have both criticized the approach in official reports. In 2011, the UN's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression expressed "alarm" from a civil liberties perspective at proposals to disconnect Internet users for violations of intellectual property rights.[64] In 2010, in connection with the ACTA negotiation process, the European Data Protection Supervisor issued a formal opinion stating that graduated response procedures for monitoring user data transmissions and identifying

---

[56] *See* Bridy, *ACTA and the Specter of Graduated Response*, *supra* note 11, at 561; Peter Yu, *Six Secret (and Now Open) Fears of ACTA*, 64 SMU L. REV. 975, 1056 (2011).

[57] Bridy, *ACTA and the Specter of Graduated Response*, *supra* note11, at 561.

[58] *Id.* at 569-70 (quoting from ACTA's final text).

[59] *Id.* at 571 (asserting that "cooperation" has become something of a code word for graduated response).

[60] Office of the United States Trade Representative, The United States in the Trans-Pacific Partnership, http://www.ustr.gov/about-us/press-office/fact-sheets/2011/november/united-states-trans-pacific-partnership (last visited March 1, 2012). The parties to the TPP are Australia, Brunei Darussalam, Chile, Malaysia, New Zealand, Peru, Singapore, Vietnam, and the United States.

[61] Trans-Pacific Partnership Agreement Intellectual Property Rights Chapter 34 (Draft of Feb. 10, 2011), http://keionline.org/sites/default/files/tpp-10feb2011-us-text-ipr-chapter.pdf (last visited March 1, 2012).

[62] See Bridy, *ACTA and the Specter of Graduated Response*, *supra* note 11, at 562-63.

[63] *See* Jacqui Cheng, *Germany Says "Nein" To Three-Strikes Infringement Plan*, ARS TECHNICA (Feb. 6, 2009), http://arstechnica.com/techpolicy/news/2009/02/germany-walks-away-from-three-strikes-internet-policy.ars (explaining the German government's decision that graduated response would be too invasive and would potentially conflict with domestic privacy laws); Howell Llewellyn, *'Three-Strikes' Off Anti-Piracy Agenda In Spain*, BILLBOARD.BIZ (June 22, 2009), http://www.billboard.biz/bbbiz/content_display/industry/e3i8071e0d9c25cb6b876d3771fb7e3d102 (reporting on the Spanish government's refusal to implement a graduated response scheme).

[64] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, at 14 (May 16, 2011).

alleged infringers to rights owners are "highly invasive" of individuals' privacy and should be abandoned in favor of less intrusive, more proportional measures.[65]

II. In the EU: Two Takes on "Three Strikes"

This Part considers two "three strikes" implementations of graduated response in two European Union (EU) countries: France and Ireland. The French system, Hadopi, has been operational since 2010.[66] Named for the government agency that administers it, its acronym translates roughly as the High Authority for the Distribution of Works and the Protection of Rights on the Internet. The Irish system, administered privately by Ireland's largest ISP, Eircom, also dates to 2010.[67] It exists and operates pursuant to the terms of a legal settlement between Eircom and members of the Irish Recorded Music Association (IRMA), which sued Eircom for secondary copyright infringement in 2008.[68] These two systems make for an interesting contrast between a public law implementation of graduated response, which was subject to constitutional scrutiny before it took effect, and a private law implementation, which was not. Significantly, neither implementation requires in-network filtering of traffic by ISPs, which is the holy grail of enforcement for the copyright industries and the most problematic potential development for consumers from the perspective of privacy and expressive rights.

A. Graduated Response as Public Law: The French Example (Hadopi)

The seeds for graduated response in France were sown in 2004, when the topic was broached in a report of France's High Council of Literary and Artistic Property.[69] The report recommended implementation of a system requiring broadband providers to send a specific number of warnings to users suspected of infringement, after which a fine would be imposed.[70] When France amended its copyright law in 2006 in compliance with EU directive 2001/29/CE, requiring harmonization of copyright law throughout the EU, it did not incorporate graduated response into the new law.[71] Rights owners persisted, however, and found a champion in President Sarkozy, who appointed a commission to develop a graduated response policy for France. In 2007, the commission submitted a report proposing the creation of an administrative body to oversee a system of warnings and sanctions for Internet users identified as repeat

---

[65] *Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement* (ACTA), 2010 O.J. (C 147) 3, 5.

[66] *Hadopi Enregistre Ses Premières Plaintes*, L'EXPRESS, July 30, 2010, http://www.lexpress.fr/actualite/politique/hadopi-enregistre-ses-premieres-plaintes_909663.html (announcing the publication of the official decree requisite for the start of operations).

[67] Eircom, Press Release, Statement on Illegal File Sharing, http://pressroom.eircom.net/press_releases/article/eircom_Statement_on_Illegal_File_Sharing/ (last visited March 1, 2012).

[68] *See* Tim Healy, *Eircom May Face Music in Illegal Files Row*, INDEPENDENT.IE, March 11, 2008, http://www.independent.ie/national-news/eircom-may-face-music-in-illegal-files-row-1313154.html (reporting on the filing of the lawsuit).

[69] *See* Thierry Rayna & Laura Barbier, *Fighting Consumer Piracy with Graduated Response: An Evaluation of the French and British Implementations*, 6 INT'L J. FORESIGHT & INNOVATION POL'Y 294, 299 (2010).

[70] *Id.*

[71] *Id.* at 300.

infringers.[72] The report was followed in 2008 by the introduction of legislation creating that administrative body, Hadopi.[73] Under the original version of the legislation, Hadopi[74] was to be responsible for implementing a graduated response system in which three warning letters would be followed by a suspension of the accused subscriber's Internet access for a maximum of one year.[75] Debate over the bill was intense both inside and outside the French parliament, with the greatest degree of controversy surrounding privacy and due process issues.[76] After passage of the bill in 2009, opponents challenged its constitutionality, and the French Constitutional Council ruled that a user's Internet access could not be suspended solely on the authority of an administrative body, without a court order.[77] To comply with the Council's ruling, the Hadopi legislation was promptly amended, and the system was reconfigured to include an accelerated legal proceeding presided over by a judge.[78] The judge has authority under the amended law to impose an access sanction without a hearing, but the affected subscriber has the right to an appeal at which he or she is represented.[79] accelerated

Notices of infringement in the Hadopi system are generated by an Internet security and content detection company selected by rights owners.[80] A notice contains relevant information concerning the alleged infringement: the IP address from which the files were available, the ISP of the alleged infringer, and the date and time of the alleged infringement.[81] The notice is forwarded from the security company to the copyright owner, which then refers the incident to Hadopi.[82] To protect the accused subscriber's privacy, Hadopi forwards the notice to the subscriber without disclosing his or her identity to the copyright owner.[83] If a subscriber is alleged to have infringed on a second occasion within six months of receiving the first notice,

interesting how they approach privacy

[72] *Id.*

[73] *Id.*

[74] The acronym translates as the High Authority for the Distribution of Works and the Protection of Rights on the Internet.

[75] Rayna & Barbier, *supra* note 69, at 301.

[76] *See* Les Députés Adoptent la Loi Hadopi, LE MONDE.FR, May 12, 2009, http://www.lemonde.fr/technologies/article/2009/05/12/les-deputes-adoptent-la-loi-hadopi_1192219_651865.html; Marguerite Reardon, France Ignores EU and Passes Antipiracy Law, CNET NEWS (May 12, 2009), http://news.cnet.com/8301-1023_3-10238912-93.html.

[77] *See* Conseil Constitutionnel [CC] [Constitutional Court] decision No. 2009-590DC, Oct. 22, 2009, Rec. 179. The original version of the law did not require judicial review. *See also* Nicola Lucchi, *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, 19 CARDOZO J. INT'L & COMP. L. 645 (2011) (discussing in detail the Council's decision and the underlying principles of French law).

[78] *See* Loi 2009-1311 du 28 Octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet [Law 2009-1311 of October 28, 2009 Regarding Criminal Protection for Intellectual Property on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O] [OFFICIAL GAZETTE OF FRANCE], Oct. 29, 2009, p. 18290; *see also* CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art. L331-21.

[79] *See* Rayna & Barbier, *supra* note 69, at 301.

[80] *Id.* at 301.

[81] *Id.*; *see also Quelles informations me concernant sont détenues par l'Hadopi si je fais l'objet d'une procédure de réponse graduée?*, HADOPI, www.hadopi.fr/faq.html (last visited Feb. 22, 2011) (explaining what information concerning an alleged infringement is transmitted to Hadopi by the copyright owner).

[82] Rayna & Barbier, *supra* note 69, at 301; *see also Réponse Graduée*, HADOPI, http://www.hadopi.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/reponse-graduee.html (last visited Dec. 8, 2010).

[83] Rayna & Barbier, *supra* note 69, at 301.

Hadopi forwards a second notice.[84] If a third infringement is alleged within a year of the second notice, Hadopi refers the matter to a prosecutor, and a judge can order the subscriber's Internet access suspended.[85] If the judge determines that the infringement was the result of a negligent failure on the subscriber's part to secure his or her Internet connection, the suspension is limited to one month.[86] If the judge determines that the infringement was not merely negligent, a one-year suspension may be imposed.[87] If the subscriber wants to contest the judge's decision to suspend access, he or she can exercise the right to be heard on appeal.[88]

Hadopi began sending notices to alleged infringers in October 2010 at a reported rate of 25,000 per day.[89] As of December 1, 2011, over 750,000 first notices had been sent.[90] According to an official report, 95% of those who received a first notice did not receive a second notice; 92% of those who received a second notice did not receive a third; and 98% of those who received a third notice had no subsequent contact with the system.[91] As of September 2012, fourteen cases had been referred for prosecution and a single fine amounting to a little under $200 had been imposed by the court.[92] Of more than 1,000 French Internet users between the ages of 15 and 50 who were surveyed in November 2011, 71% of those who used P2P networks stated that they would stop downloading content illegally if they received a notice from Hadopi.[93] These figures suggest that Hadopi notices are having a meaningful deterrent effect on their recipients.

With respect to Hadopi's effect on file-sharing, the official report cites a study finding a 43% drop in illegal file sharing in France in 2011 and a drop in France's contribution to global illegal file-sharing in 2011 from 6.2% to 4.5%.[94] Hadopi attributes these decreases to its own success as a deterrent, but the numbers can as plausibly be attributed, at least in part, to an increase in illegal streaming and direct download (DDL) traffic, both of which use non-P2P transmission protocols.[95] When increased illegal streaming and direct download traffic are taken

---

[84] *Id.* (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art. L331-25); *see also Comment fonctionne la réponse graduée?*, HADOPI, www.hadopi.fr/faq.html (last visited Feb. 23, 2011) (explaining the protocol).

[85] Rayna & Barbier, *supra* note 69, at 301 (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art L335-7); *see also Comment fonctionne la réponse graduée?*, *supra* note 84.

[86] This can occur, for example, in a situation where the subscriber is a parent whose child is the accused infringer. *See* Rayna & Barbier, *supra* note 69, at 301 (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art. L335-7-1); *Qu'est-ce que l'infraction de négligence caractérisée?*, HADOPI, www.hadopi.fr/faq.html (last visited Feb. 22, 2011).

[87] Rayna & Barbier, *supra* note 69, at 301. During this period, the subscriber remains responsible for the regular price of the subscription and may not subscribe to another service. *Id.* at n.13.

[88] *Id.* at 301–02.

[89] Aymeric Pichevin, *French Anti-Piracy Scheme's 25,000 Daily Reports*, BILLBOARD.BIZ, Oct. 22, 2010.

[90] *See* Hadopi, HADOPI: 11/2 YEAR AFTER THE LAUNCH 3 (2012), available at http://www.hadopi.fr/sites/default/files/page/pdf/note17_en.pdf.

[91] *Id.*

[92] *See* Peter Sayer, *French Court Levies First Fine Under Three-strikes Law on Illegal Downloads*, PCWORLD, Sept. 13, 2012, https://www.pcworld.com/article/262285/french_court_levies_first_fine_under_threestrikes_law_on_illegal_downloads.html.

[93] Hadopi, *supra note 90,* at 6.

[94] *Id.* at 5.

[95] *See* Benjamin Ferran, *Le Bilan Contrasté de l'Action de l'Hadopi*, LE FIGARO, Mar. 28, 2012, http://www.lefigaro.fr/hightech/2012/03/27/01007-20120327ARTFIG00670-le-bilan-contrastee-de-l-action-de-l-

B. Graduated Response as Private Law: The Irish Example (Eircom)

In contrast with the government-administered system in France, Ireland's graduated response system is privately administered. As with CAS, the legal basis for the Irish system is a contractual arrangement between private parties: Ireland's largest ISP, Eircom, and members of the Irish Recorded Music Association (IRMA). Unlike the MOU, however, which was negotiated outside the context of litigation, the agreement that produced the Eircom graduated response system was an agreement to settle a lawsuit alleging secondary copyright infringement.[104] After an eight day trial, the parties agreed in 2009 to a settlement that required Eircom to implement a "three strikes" protocol.[105] The case never went to judgment on the merits, so there is no copyright law on the books as a result of it,[106] yet the settlement has the reach and effect of public law: every one of Eircom's 2.6 million subscribers is now bound through Eircom's Terms of Service to the terms of the Eircom-IRMA settlement.

The Eircom protocol was implemented on a preliminary basis beginning in June 2010 and on a permanent basis the following October.[107] Upon receiving a first notice of infringement from a computer security firm hired by IRMA to monitor P2P networks for infringing content, Eircom informs its allegedly infringing subscriber that s/he has been caught in the act of illegal uploading or downloading.[108] This first warning is included with the subscriber's monthly bill.[109] Upon receipt of a second notice of infringement concerning the same subscriber, Eircom sends a separate letter to the subscriber that contains a strongly worded warning.[110] The response escalates from the first level to the second level only if fourteen days or more have passed since the first infringement was alleged.[111] Upon receipt of a third notice concerning the same subscriber, Eircom reviews the evidence against the subscriber. As with the escalation from the first level of response to the second, fourteen days or more must pass before the response can graduate to the third level.[112] The first two notices are generated automatically; the third notice, however, triggers a human review. Following human review, a notice of termination is sent to the subscriber, who has fourteen days to respond.[113] Eircom considers the response, if any is received, in light of any extenuating circumstances the subscriber raises. If the subscriber claims in his or her response that there was a mistake of fact concerning the alleged infringements, Eircom considers that claim as well.[114] If Eircom does not find in favor of the subscriber, the

how do they consider?

---

[104] *See* EMI Records v. Eircom Ltd., [2010] IEHC 108 (H. Ct.) (Ir.).

[105] *See id. at* ¶¶ 2, 9.

[106] In a subsequent case, IRMA sought a court order requiring UPC, another Irish ISP, to implement a graduated response system like Eircom's. EMI Records v. UPC Communications, [2010] IEHC 377 (H. Ct.) (Ir.). The Court denied the requested relief, pointing out that the agreement between Eircom and IRMA was not Irish law but "a private matter between the parties as a matter of contract…[that] was not authori[z]ed or ruled on by the Court." *Id.* at ¶¶ 5-6.

[107] *See* Press Release, Eircom, Eircom Statement on Illegal File Sharing (December 8, 2010) (http://pressroom.eircom.net/press_releases/article/eircom_Statement_on_Illegal_File_Sharing/); IFPI Digital Music Report, *supra* note ___, at 18.

[108] *EMI Records*, [2010] IEHC at ¶ 9.

[109] *Id.* ¶ 13.

[110] *Id.* ¶¶ 9, 13.

[111] *Id.* ¶ 13.

[112] *Id.*

[113] *Id.*

[114] *Id.*

into account, it is not so clear that the drop in P2P traffic observed in the study corresponds directly to a drop in online infringement. Users could just be migrating to different methods of online infringement—ones that the Hadopi system is unequipped to detect and mitigate. Another plausible alternative explanation for at least some of the observed decrease in P2P traffic is increased reliance on virtual private networks and encryption by P2P users seeking to evade detection by the monitors feeding information to Hadopi.[96] When these alternative explanations are considered, the argument that Hadopi has dramatically decreased the volume of online infringement loses some of its force.

Another way of measuring the impact of Hadopi on French consumer behavior is to study the law's effect on legal music sales, which is what a team of American researchers led by the economist Brett Danaher did.[97] Danaher and his co-authors concluded that public awareness of Hadopi drove French consumers to legal (iTunes) downloads.[98] Relying on data from the "big four" recording labels—EMI, Sony, Universal, Warner—and using sales trends in a selected group of European countries as a proxy for what sales would have been in France if Hadopi had not been enacted, the authors reported that public awareness of Hadopi caused a 25% increase in iTunes album sales in France.[99] It remains to be seen however, whether the increased digital sales observed in the study will be sustained when Hadopi is no longer a focus of media attention in France, as it was for a significant period of time both before and after the law became effective.[100] Past studies on the effects of highly publicized file-sharing lawsuits against individual downloaders in the United States showed only a short-term impact on illegal file-sharing behavior.[101] Danaher and his co-authors assert that Hadopi will be more effective than lawsuits at achieving long-term general deterrence, but their data do not go beyond May 2011, which is only about six months after the first Hadopi notices were sent.[102] It also remains to be seen whether Hadopi will be somehow reconfigured under the presidency of Sarkozy's successor, the socialist François Hollande, who called for repeal during the presidential campaign but has since moderated his position.[103]

---

hadopi.php (citing a 29% rise in Internet traffic to illegal streaming and direct download sites since Hadopi began sending notices to P2P users in October 2010).

[96] *See* Monica Horten, *Hadopi—Has It Massaged the Numbers?,* IPTegrity.com Blog, March 31, 2012, http://www.iptegrity.com/index.php/france/755-hadopi-has-it-massaged-the-numbers (stating that France Telecom noted a "marked increase" in encrypted traffic following the first round of Hadopi notices); Eric Pfanner, *Copyright Cheats Face the Music in France*, NY TIMES, Feb. 19, 2012, https://www.nytimes.com/2012/02/20/technology/20iht-piracy20.html?_r=1 (discussing the increased use of virtual private networks and anonymous browsing following Hadopi).

[97] *See* Brett Danaher *et al.*, *The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240.

[98] *Id.* at 2.

[99] *Id.*

[100] Using a difference-in-difference model, the authors estimated effects over a one year time period—six months before and six months after the law became effective. *See id.* at 16 n.16.

[101] *E.g.,* Michael Bachmann, *Lesson Spurned? Reactions of Online Music Pirates to Legal Prosecutions by the RIAA*, 1 INT'L J. CYBER CRIMINOLOGY 213, 220 (2007) (concluding that an upward trend in downloading across all demographic groups between 2003 and 2005 suggests that the deterrent effect of the RIAA's lawsuits eroded over time).

[102] *See* Danaher, et al., *supra* note 96, at 2, 20-21.

[103] *See, e.g.,* Christophe Auffray, *Hadopi "Repensée." Mais Que Veut Finalement François Hollande?*, ZDNET.FR, Mar. 2, 2012, http://www.zdnet.fr/actualites/hadopi-repensee-mais-que-veut-finalement-francois-hollande-39769220.htm (reporting on the shift in Hollande's views concerning Hadopi).

subscriber's Internet service is cut off for seven days.[115] If the user continues to infringe, his or her service is disconnected for a year.[116] No court order is required; the ISP is the sole arbiter of innocence or guilt.[117]

As of December 2011, Eircom had issued 29,000 notices to its subscribers under the protocol.[118] One hundred subscribers had reached the point of a seven-day suspension, and only 12 had reached the point of receiving a longer suspension.[119] The dramatic drop-off in the number of subscribers progressing from one stage of the protocol to the next is consistent with statistics from Hadopi. But unlike in France, where opposition to the Hadopi legislation in its initial form resulted in amendments designed to ensure judicial review of disconnection decisions, Eircom's subscribers have no such guarantee. In this respect, privately designed and implemented graduated response protocols like Ireland's (and CAS) are more problematic from the standpoint of consumer protection than publicly implemented ones. To the extent that these regimes implicate rights and privileges protected by public law, waivers of those rights by users via "click through" standardized terms of service are legally enforceable, even if users have no choice of an alternative provider offering service on different terms.[120] By signing up for broadband service, Eircom's subscribers consent to graduated response and surrender any conflicting public law guarantees.[121]

The graduated response system spawned by the Eircom-IRMA settlement has not escaped legal challenges, however, including two regulatory interventions by Ireland's Data Protection Commissioner alleging subscriber privacy violations. In 2010, on the heels of the settlement, the Commissioner expressed the opinion that the settlement terms violated Irish data protection laws, prompting the Irish High Court to rule that copyright owners' collection of subscribers' Internet Protocol (IP) addresses during surveillance of P2P networks is lawful.[122] The Court also ruled that the Eircom protocol contains adequate procedural protections and that Internet disconnection after three strikes is a proportional and justified restraint on fundamental freedoms relating to Internet access.[123] Not considering the matter closed, the Commissioner acted again at the end of 2011, following a six-month investigation of consumer complaints arising from an incident in which 390 subscribers were misidentified as infringers due to what

---

[115] Press Release, *supra* note 105 (setting forth sanctions under the protocol).

[116] *Id.*

[117] *See EMI Records*, [2010] IEHC at ¶¶ 14-15 (characterizing the protocol and its sanctions as consistent with Eircom's terms of service regarding the suspension or termination of accounts).

[118] Mark Tighe, *Eircom Cut Off 100 Illegal Downloaders*, SUN. TIMES (LONDON), Mar. 4, 2012, at 5.

[119] *Id.*

[120] The validity of consumers' assent to the "fine print" in mass standardized agreements has been the subject of considerable scholarly debate, particularly when the terms are presented virtually in "clickwrap" or "browsewrap" form. *Compare, e.g.,* Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459 (2006) (discussing the "death of assent" in mass digital contracts), *with* RANDY E. BARNETT, *Consenting to Form Contracts*, *in* PERSPECTIVES ON CONTRACT LAW 171, 184 (2009) (arguing that even "invisible" terms in mass contracts can be justifiably enforced on the basis of "real consent properly understood"). *See also* Margaret Jane Raden, *Regulation by Contract, Regulation by Machine*, 160 J. INSTITUTIONAL & THEORETICAL ECON. 142 (2004) (examining and critiquing the rise of mass contract regimes through which the law of the state is superseded by the law of the firm).

[121] *See, e.g., EMI Records*, [2010] IEHC at ¶ 29 ("The insertion of express conditions by Eircom in the user–internet service provider contract…is no less than lawful and proper. It is abundantly clear that the [user] has given his or her consent in return for obtaining internet access.").

[122] *EMI Records*, [2010] IEHC at ¶¶ 18, 25.

[123] *Id.* at ¶ 27.

Eircom characterized as a "minor technical issue."[124] In an enforcement notice, the Commissioner accused Eircom of, among other things, facilitating surveillance of users' Internet traffic without their consent, improperly retaining and using data linking users' identities to dynamically assigned IP addresses, and failing to ensure the accuracy of that data.[125] The notice concluded with an order for Eircom to stop administering the protocol.[126] IRMA's member companies promptly appealed the order, arguing that it represented an attempt to re-litigate the data protection issues already decided by the High Court in 2010.[127] In June 2012, the High Court invalidated the order because the accompanying enforcement notice failed to state an explicit legal rationale for the Commissioner's action.[128] To the extent that a rationale could be discerned in the notice, the court held, it rested on a misconstruction of the applicable law.[129] Following an extended discussion of European Court of Justice (ECJ) precedents, and stressing the need to balance the competing rights of Internet users and intellectual property owners in the digital environment, the court concluded that accepting the Commissioner's interpretation of EU privacy law would require a holding that copyright may not be enforced on the Internet.[130]

III. In the US: Six Strikes (But You're Probably Not Out)

This Part describes in detail the substance of the graduated response MOU. Subpart A summarizes the provisions creating the Center for Copyright Information (CCI), which is the co-governed private entity charged with macro-level administration and oversight of the Copyright Alert System (CAS). Subpart B explains CAS itself, which is comprised of a standardized notice-and-sanction protocol and a coordinating process of third party non-judicial review.

A. The Center for Copyright Information (CCI)

The establishment of CCI is the first order of business addressed in the MOU. As a public-facing entity, CCI is tasked primarily with educating a general audience about copyright law, the problem of online infringement, and legal sources of online content.[131] It does this by means of a website to which the parties to the MOU contribute materials reflecting their perspective on the problem and their proffered solutions.[132] As the center of gravity for the inter-

[124] Mary Carolan, *Four Music Firms Dispute Data Chief's Notice to Eircom*, IRISH TIMES, Mar. 1, 2012, at 4. Eircom did not change the clocks in its network to reflect daylight savings time until December 2010, two months late. EMI Records v. Eircom, [2012] IEHC 164, ¶ 1.0. This mistake caused a mismatch of dynamically assigned IP addresses to subscriber accounts and led to the delivery of erroneous notices of infringement. *Id.* at ¶ 1.3.

[125] Data Protection Commissioner's Enforcement Notice to Eircom Ltd. Pursuant to Section 10 of the Data Protection Acts 1988 & 2003 and Regulation 17 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, Dec. 5, 2011 (on file with author).

[126] Mark Tighe, *Piracy Action Lands Eircom in Hot Water*, SUN. TIMES (London), Dec. 18, 2011, at 7.

[127] Carolan, *supra* note 122, at 4.

[128] *EMI Records*, [2012] IEHC at ¶ 14.0.

[129] *Id.*

[130] *See id.* at ¶ 8.10 ("To sum up, it is clear that the state of the law was regrettably misconstrued by the Data Protection Commissioner. In that respect, he is not to be faulted as the law is complex. The law does not, however, set intellectual property rights at naught because of the involvement of the Internet.").

[131] MOU, *supra* note 12, at 3.

[132] *Id.*

industry partnership created by the MOU, CCI is also charged with assisting in the implementation and oversight of CAS and with promoting CAS to non-participating ISPs.[133]

Reflecting the delicate balance of corporate interests involved in the MOU and its common framework for graduated response, contractual rights and duties concerning CCI are allocated equally between the participating ISPs and copyright owner representatives. Funding for CCI is split 50-50, and the organization is governed by a six-member executive committee of which each group chooses three members.[134] There is no public interest or copyright expert representation on the executive committee; however, the MOU requires the formation of a three-member advisory board to be "drawn from relevant subject matter expert and consumer interest communities."[135] Under the terms of the MOU, each group appoints one member of the advisory board, and those two members together choose the third member.[136] The executive committee is required to consult the advisory board on significant issues relating to the design and implementation of CAS, but the advisory board has no power to make binding recommendations.[137] As Mary LaFrance has observed, the MOU provides no real guarantee that the advisory board will have any direct impact on CCI's activities.[138]

Members of the CCI's inaugural advisory board, which actually has four members instead of the anticipated three, include Jerry Berman of the Center for Democracy and Technology and Gigi Sohn of Public Knowledge.[139] The other two members are Marsali Hancock, the president of the iKeepSafe Coalition, which monitors digital technologies and their effect on children, and Jules Polenetsky of the Future of Privacy Forum.[140] Berman and Sohn are nationally known Open Internet advocates whose organizations have long emphasized the need for balance in the protection and enforcement of digital copyrights.[141] All four appointees have solid public interest credentials and occupy positions of genuine independence from the parties. The appointments are a strong signal to the public that the parties to the MOU are actually serious about the need to balance systematic enforcement with consumer protection.

In addition to appointing an advisory board, the CCI executive committee is required to retain independent technical experts and privacy experts to review the methods used by participating copyright owners to identify infringers and infringing content on P2P networks.[142] According to the MOU, the retention of experts is intended to ensure and maintain the parties'

---

[133] *Id.*
[134] *Id.* at 3-4.
[135] *Id.* at 4.
[136] *Id.* at 3.
[137] MOU, *supra* note 12, at 4.
[138] Mary LaFrance, *Graduated Response by Industry Compact: Piercing the Black Box*, 30 CARDOZO ARTS & ENT. L.J. 165, 171 (2012).
[139] Press Release, *supra* note 129.
[140] *Id.*
[141] *See, e.g.*, CDT, Digital Copyright, https://www.cdt.org/issue/digital-copyright (last visited June 13, 2012) (asserting that "concern over copyright infringement does not justify policies that jeopardize the open architecture of the Internet or stifle innovation or legitimate free expression"); Public Knowledge, Key Issues: Balanced Copyright, http://www.publicknowledge.org/issues/balanced-copyright (last visited June 13, 2012) ("Public Knowledge promotes a balanced approach to copyright law and works to ensure that domestic and international copyright laws promote creativity and the free flow of knowledge.").
[142] MOU, *supra* note 12, at 5.

and the public's confidence in the accuracy and security of those methods.[143] Like the recommendations of the advisory board, however, any recommendations these experts make are confidential and non-binding.[144] The incentive created in the MOU for copyright owners to follow expert technical recommendations is a prohibition on sending notices of infringement to ISPs if the notices were generated using "fundamentally unreliable" methods.[145] As of this writing CCI has not publicly identified its independent experts, but some news reports have attributed delays in the launch date for CAS to an ongoing process of independent technical review.[146]

B. The Copyright Alert System (CAS)

The MOU contains a complete procedural specification for CAS but leaves the operational details to CCI, working in consultation with the parties, the advisory board, and the independent experts. While the details are legion, the basic bargain struck in the MOU is straightforward: Copyright owners agree to identify and provide ISPs with documented evidence of suspected individual infringements over P2P networks.[147] ISPs agree, in turn, to match detected instances of infringement with subscriber accounts, send warnings to the relevant subscribers, and impose sanctions on subscribers who fail to heed repeated warnings.[148] The overarching goal, and perhaps the greatest operational challenge associated with CAS, is standardization of the system across ISPs. Each ISP is responsible for establishing its own implementation plan and for taking that plan operational on a target launch date.[149] Each ISP is also required to modify its terms of service for residential broadband to incorporate the notice-and-sanction structure of CAS.[150] As with the Eircom graduated response system, the CAS protocol becomes binding on broadband subscribers through standardized terms of service, i.e., the law of contracts.

1. The Six Strikes Protocol

At the core of the CAS protocol is an escalating sequence of six warnings, or "copyright alerts," separated by seven day grace periods.[151] To begin the process, a copyright owner sends a notice of infringement to a subscriber's ISP, which then generates an alert and sends it to the subscriber whose IP address was identified in the notice.[152] To prevent ISPs from being overwhelmed by an unmanageable volume of notices, the MOU requires participating copyright owners to allocate among themselves an unspecified (but presumably fixed) number of notices per month.[153] In addition to that limit, ISPs have discretion to temporarily stop processing notices

---

[143] *Id.*

[144] *Id.*

[145] *Id.* at 6. Whether that is a strong enough incentive will be addressed in Part IV below.

[146] *See, e.g., US "Six Strikes" Anti-Piracy Scheme Delayed*, TORRENTFREAK (May 18, 2012), https://torrentfreak.com/us-six-strikes-anti-piracy-scheme-delayed-120518/.

[147] MOU, *supra* note 12, at 4.

[148] *Id.* at 4-5.

[149] *Id.* at 7.

[150] *Id.*

[151] MOU, *supra* note 12, at 7. An ISP may send additional alerts during grace periods, but those alerts do not count toward the total number of six. *Id.* at 10.

[152] *Id.* at 7.

[153] *Id.* at 16.

if the demand on their systems and resources becomes unreasonable.[154] Any temporary stoppage must be followed, however, by prompt notice to copyright owners and a collaborative effort to correct the "over-provisioning."[155]

The first two copyright alerts are educational in nature and require no response or action from the subscriber.[156] They explain that copyright infringement is illegal, that there are lawful ways of obtaining copyrighted content, and that users who persist in infringing copyrights will be subject to sanctions.[157] The third and fourth alerts contain sterner language and require the subscriber to take affirmative action to acknowledge receipt.[158] The required acknowledgment can occur by means of either a click-through pop-up window or a click-through landing page to which the user's browser is diverted.[159] At the acknowledgment stage, the subscriber must indicate that he or she agrees to immediately stop any infringing conduct in which he or she may have been engaged.[160]

Sanctions, or "mitigation measures," are not triggered until a fifth alert is sent.[161] The MOU avoids being prescriptive when it comes to sanctions, specifying instead a range of mitigation measures from which ISPs can choose. Such measures include, but are not limited to, a temporary reduction in transmission speed, a temporary step-down in the subscriber's service tier, a temporary redirection to a landing page for completion of a program of copyright instruction, a temporary redirection to a landing page until the subscriber contacts a customer service representative, or a temporary suspension of access.[162] No ISP operating under the MOU is required to suspend access for any subscriber. (This point should be emphasized, because it upsets the common assumption that Internet disconnection is always the end-game in graduated response.) In lieu of imposing a mitigation measure with the fifth alert, the ISP may elect to waive the measure and send a standalone fifth warning alert.[163] The sixth alert, however, must be accompanied by some mitigation measure.[164] The mitigation measure can be the same one that was applied with the fifth alert, assuming the sanction was not waived at that stage, or a different one.[165] After the sixth alert has been sent, the ISP has no further obligation to continue sending alerts to the subscriber, but it is required to keep count of any additional notices received from copyright owners concerning that subscriber.[166] At every stage, the system will "reset" for the subscriber if 12 months pass without the receipt of an additional alert.[167]

---

[154] *Id.*
[155] *Id.*
[156] *Id.* at 8. An ISP may reduce the number of educational alerts from two to one, at its discretion. *Id.*
[157] MOU, *supra* note 12, at 8.
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.* at 10-11.
[162] *Id.* at 11.
[163] MOU at 12.
[164] *Id.*
[165] *Id.* at 12-13.
[166] *Id.* at 13.
[167] *Id.*

2. The Appeal Process

Before any mitigation measure is imposed, the recipient of a fifth or sixth alert has fourteen days to appeal the alert via a non-judicial process outlined in the MOU.[168] The appeal process, which the MOU calls the "Independent Review Program," is a non-exclusive dispute resolution system administered by the American Arbitration Association (AAA) under contract with CCI.[169] Overall costs of administration are split between the copyright owner representative and ISP groups.[170] At the individual case level, an appealing subscriber pays a $35 filing fee, which may be waived at the discretion of AAA.[171] The filing fee is refundable if the subscriber prevails in his or her appeal. The appeal process is designed to be "automated to the maximum extent practicable."[172]

Each appeal is decided by a single reviewer chosen by AAA from a panel of neutrals.[173] Reviewers must be lawyers, but they are not required to have the level of legal and case management experience that AAA arbitrators deciding other kinds of cases have.[174] All reviewers deciding CAS appeals are trained by a AAA-commissioned, CCI-approved copyright expert to apply prevailing legal principles as determined by federal courts.[175] By the terms of the MOU, this copyright expert must agree to receive input from copyright owners concerning what the prevailing legal principles are.[176]

A subscriber initiates an appeal by completing an online form wherein the subscriber asserts a defense or defenses to the allegations in the alert. The MOU limits a subscriber's grounds for review to exactly six: (1) account misidentification; (2) unauthorized use of account; (3) authorized use of content; (4) fair use; (5) misidentification of content; and (6) work published before 1923. No other defenses are mentioned in the MOU, although a number of other defenses to copyright infringement claims are available to defendants in civil cases brought under the Copyright Act. With respect to each of the six possible grounds for review, the burden of proof is on the subscriber, effectively creating a presumption of infringement. That is to say, a sanction will be imposed unless the subscriber wins the appeal.

In cases where the subscriber alleges *account misidentification*, two types of error can come into play: incorrect capture of a subscriber's Internet protocol (IP) address and incorrect matching of a captured IP address to a subscriber's account.[177] The copyright owner or its agent

---

[168] *Id.* at 14.

[169] *Id.* at 26; Press Release, *supra* note 129 (announcing that AAA is the entity that will conduct independent reviews).

[170] MOU, *supra* note 12, at 14.

[171] *Id.* at 30.

[172] *Id.* at 34.

[173] *Id.* at 31.

[174] *Id.* at 33.

[175] *Id.* at 35.

[176] *Id.*

[177] An example of incorrect capture is illustrated in a 2008 study by computer science researchers at the University of Washington, who were able to trick P2P network monitors into sending notices of infringement to printers and other networked devices incapable of being used to share files. *See* Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks–or–Why My Printer Received a DMCA Takedown Notice*

is the source of the first type of error; the ISP is the source of the second. With respect to address capture errors, copyright owners under the MOU enjoy a rebuttable presumption of correctness as long as their method of capturing IP addresses was not found to be "fundamentally unreliable" by the CCI's independent technical expert.[178] In cases where the subscriber alleges *misidentification of content*, copyright owners are likewise entitled to a rebuttable presumption of correctness as long as their method of identifying their copyrighted content has not been found "fundamentally unreliable."[179] When it comes to defenses involving misidentification, any method of IP address capture or content identification that is not "fundamentally unreliable" is treated as adequate under the MOU.[180]

A subscriber may invoke the defense of *unauthorized use of account* only if the unauthorized user was not a member or invitee of the subscriber's household, making the subscriber ultimately sanctionable for any infringements that occur under his or her roof.[181] The unauthorized use scenario for which the defense is intended occurs when a subscriber's wireless router is left unsecured or is hacked, and strangers thereby gain access to the subscriber's home network and Internet connection.[182] An additional limit on the unauthorized use defense is that it may be used only once per subscriber, after which the subscriber is expected to secure his or her router to prevent future unauthorized use.[183] This *de facto* security obligation arises whether or not the subscriber has any contractual obligation to his or her ISP to secure his or her router.[184]

In cases where the subscriber alleges *authorized use of content*, the subscriber bears the burden of producing credible written evidence of specific authorization by the copyright owner or someone authorized by the copyright owner to reproduce the file in question.[185] A subscriber raising a defense of authorized use may have his or her identity disclosed to the copyright owner if such disclosure is necessary for the claim of authorization to be evaluated.[186] This is the only circumstance in which a subscriber's identity may ever be disclosed to a copyright owner within

---

(Univ. of Wash. Technical Report No. UW-CSE-08-06-01, 2008), *available at* http://dmca.cs.washington.edu/dmca_hotsec08.pdf.

Incorrect matching can occur in cases where ISPs assign IP addresses dynamically, from a pool, as individual users connect to the Internet. Over the course of time, the same IP address is assigned to different subscribers, creating the potential for mismatches if there are errors in the ISP log files that keep track of IP address assignments. *Cf.* Saul Hansell, *Google Says IP Addresses Aren't Personal*, NY TIMES (February 22, 2008, 5:16 pm), http://bits.blogs.nytimes.com/2008/02/22/google-says-ip-addresses-arent-personal/.

[178] MOU, *supra* note 12, at 5, 27.

[179] *Id.* at 5, 28.

[180] *Id.* at 5 (providing that a confidential "finding of inadequacy" shall be issued if the method of identification is found to be "fundamentally unreliable").

[181] *Id.* at 27.

[182] *Id.*

[183] *Id.* The subscriber may raise the defense more than once only if s/he shows by clear and convincing evidence that s/he took reasonable steps to secure the account following the first occurrence of unauthorized use. *Id.*

[184] Although copyright owners have argued that a user's failure to secure his or her router constitutes actionable negligence, courts have held that there is no tort duty for broadband users to secure their routers. *See* Liberty Media Holdings, LLC v. Tabora, No. 12 Civ. 2234, 2012 WL 2711381, *2 (S.D.N.Y. July 9, 2012); AF Holdings, LLC v. Doe, No. C 12–2049 PJH, 2012 WL 3835102, *4 (N.D.Cal., Sept. 4, 2012) (both cases holding that a negligence claim for failure to secure a router used by a direct copyright infringer is preempted by the Copyright Act).

[185] MOU, *supra* note 12, at 27.

[186] *Id.* at 29.

the structure of CAS.[187] In all other cases, the subscriber's identity is known only to the ISP and the reviewer.

The remaining defenses—*fair use* and *publication before 1923*—derive from specific provisions of the Copyright Act.[188] The merits of a subscriber's fair use defense are determined pursuant to prevailing legal principles as determined by CCI's approved expert.[189] To avoid hairsplitting over cases of *de minimis* use, copyright owners agree in the MOU to focus only on file transfers that involve transmission of a complete or substantially complete copyrighted work.[190] Decisions about what constitutes a "substantially complete" copy of a work appear to be left to copyright owners.[191] The final ground for appeal—that the work was published before 1923—relates to copyright's limited duration (i.e., no work published before 1923 is still protected by copyright) and amounts to a claim that the work in question is in the public domain because its copyright has expired.[192] The burden of demonstrating publication before 1923 falls on the subscriber.[193] Although there are other reasons for which a work may be in the public domain, none of them is available as a defense in the review process laid out in the MOU.[194]

When asserting one or more of the six cognizable grounds for review, the subscriber must provide sufficient factual information to allow the reviewer to evaluate the merits of the defense(s).[195] Once an appeal has been initiated, the reviewer is also provided with a standard package of information concerning the subscriber's contacts with CAS leading up to the appeal.[196] The reviewer may request supplemental information from the copyright owner or the ISP if such information is needed to decide the appeal.[197] Beyond requests for supplemental information, the MOU provides that there be no communication concerning pending appeals among the reviewer, the ISP, and the copyright owner.[198] The entire appeal process is designed to be completed within 10 days of the reviewer's receipt of a complete file and within about 30 days of the initiation of the appeal.[199] If the subscriber prevails, the copyright alert in question is invalidated.[200]

IV. Five Norms for Measuring Six Strikes

The implementation of privately designed and administered graduated response protocols like CAS raises a host of public interest concerns, five of which are the focus of this Part:

---

[187] MOU, *supra* note 12, at 14.
[188] *See* 17 U.S.C. § 107 (fair use); 17 U.S.C. §§ 302-304 (duration).
[189] MOU, *supra* note 12, at 35.
[190] *Id.* at 6.
[191] *See* LaFrance, *supra* note 136, at 174. As Professor LaFrance points out, even a large amount of copying can fall under the rubric of fair use when, for example, the use is for parody. *Id.*
[192] *See* MOU, *supra* note 12, at 28.
[193] *Id.*
[194] Some of these reasons are discussed in Part IV. C infra.
[195] *Id.* at 29.
[196] MOU, *supra* note 12, at 31-32.
[197] *Id.* at 32.
[198] *Id.* at 34.
[199] *Id.* at 31-35 (prescribing deadlines for successive phases of the review process).
[200] *Id.* at 28.

freedom of expression, privacy, fairness, proportionality, and transparency. Although the same concerns are raised by publicly administered protocols like Hadopi, the private nature of CAS means that there will be no public forum for debate over the terms of the MOU or the procedures and sanctions it prescribes. CAS was presented to the public as a *fait accompli* and will be offered for the public's assent as a contract of adhesion for broadband service. There will be, in other words, no bargaining about it. Some people will be able to choose a non-party ISP[201] and thereby avoid being subject to CAS, but many (if not most) will not have that option given the state of the market for residential broadband service and the size and reach of the ISPs participating in the MOU.[202] CAS will be the law for millions of U.S. broadband subscribers, whether they like it or not. As with the Eircom protocol, because there is no state action involved, there will be no judicial review of the constitutionality of the MOU's provisions. The CCI advisory board, whose members were not even appointed until after negotiations over the substance of CAS were closed, is the public's only advocate within the CAS governance structure, yet it had no role in the design of the protocol and is not empowered to make recommendations about implementation that bind the CCI executive committee. What follows is a public interest assessment of CAS, which reveals that the protocol is a mixed bag for broadband users.

public pressure

A. Freedom of Expression

The two most significant threats to freedom of expression in online copyright enforcement are suspension of Internet access, which is the typical endpoint of graduated response protocols, and content filtering, which ISPs can do using deep packet inspection (DPI) technology already deployed within their networks for traffic management and other purposes.[203]

1. Suspension of Access

should read more about use of DPI

Of the two threats, suspension of access, which can be either across-the-board or service-selective, is the more extreme. Across-the-board suspension of access forecloses all online communication for affected subscribers and their households for the duration of the suspension. For subscribers who bundle broadband Internet access and VOIP telephony into one package, across-the-board suspension of access entails the loss of phone service in addition to the loss of Web access and Web-reliant applications like media streaming and video conferencing. In contrast, a service-specific suspension of access might block access to the World Wide Web but leave other services, including telephony and e-mail, unaffected. The extent to which a suspension of access impinges on expressive freedoms will vary with the duration of the suspension and the range of affected services: the longer and more comprehensive the suspension, obviously, the greater its impact.

that is big

though very small #

- but certain protocols → NN

[201] Cox. Qwest, RCN, CableOne, Charter, and Mediacom, for example, are not parties to the MOU.

[202] In 2010, the Federal Communications Commission (FCC) reported that 96% of the U.S. population had at most two wireline broadband providers from which to choose. *See* FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 37 (2010). To unpack that statistic, approximately 4% of households were served by three providers, 78% were served by two, 13% were served by one, and 5% had no access to wireline broadband. *Id.*

[203] *See* Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at 104-105 (discussing the various uses of deep packet inspection).

Both types of suspension impact expressive freedoms beyond freedom of speech, including freedom of association, freedom to receive information, and freedom to engage in commercial transactions. In a world that depends increasingly on the Internet for all kinds of meaningful social, cultural, political, and commercial activity, suspension of access is a sanction laden with consequences that reach far beyond the consumption of copyrighted content and the ability to swap files over P2P networks.[204]

The MOU permits but does not require participating ISPs to suspend access for subscribers reaching the fifth or sixth copyright alert.[205] As discussed above in Part III.B, temporary suspension of access is one among many mitigation measures from which ISPs can choose in order to comply with their obligation to sanction. Permanent disconnection is not contemplated at all, and ISPs retain the right under the MOU to be service-selective in their suspensions, excluding services like telephony, e-mail, and multi-channel video programming.[206] Given the menu of lesser measures available and the draconian flavor of suspension of access, it would be surprising to see ISPs voluntarily taking that route under CAS, even in a service-selective and time-limited way. To attract and retain customers, participating ISPs have an incentive to gravitate toward the more moderate, user-friendly sanctions enumerated in the MOU (e.g., "copyright school," customer service contact, or temporary speed or service tier reductions), which they will almost certainly do. This prediction jibes with a public statement from CCI's director, Jill Lesser, who said in an interview that termination is not an anticipated sanction because the ultimate aim of CAS is educational and not punitive.[207]

2.- Content Filtering

The second major threat to expressive freedom in graduated response regimes is in-network filtering of infringing content. During the legislative process that led to the creation of Hadopi in France, corporate copyright owners pushed hard for a filtering mandate, but their efforts failed, in large part over concerns about compromising expressive rights guaranteed in the European Convention on Human Rights.[208] On this side of the Atlantic, filtering has been an open topic of conversation between corporate copyright owners and US-based ISPs since at least 2008, but the major ISPs have so far declined to do it, citing the need for improvements in the technology and the need to find a consumer friendly approach.[209]

Filtering threatens freedom of expression because of the potential for over-blocking, which has not been (and possibly may never be) reliably eliminated through improvements in

---

[204] *Id.* at 126.

[205] *See* MOU, *supra* note 12, at 11 (listing "temporary restriction of the Subscriber's Internet access for some reasonable period of time" among possible mitigation measures).

[206] *Id.* at 12.

[207] *See* Sarah Lai Stirland, *The Center For Copyright Information's New Chief Jill Lesser On Top ISPs' New "Copyright Alert" System*, TECHPRESIDENT, Apr. 5, 2012, http://techpresident.com/news/22016/interview-center-copyright-informations-new-chief-jill-lesser (interviewing Jill Lesser).

[208] *See* HORTEN, *supra* note 46, at 49-51 (discussing the right to freedom of expression under European law) and 89 (quoting from copyright industry submissions to EU governmental entities in support of a filtering mandate for ISPs).

[209] *See* Brad Stone, *AT&T and Other I.S.P.'s May Be Getting Ready to Filter*, NY TIMES (Jan. 8, 2008, 7:07 pm), http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/ (reporting on the subject matter of a panel discussion on digital piracy at the 2008 Consumer Electronics Show).

technology. Copyright infringing speech is not protected under the First Amendment, but separating it from protected speech as it whips through cyberspace in tiny packets is a tall order. Even when methods for identifying unauthorized files in transit are highly accurate, the computer algorithms on which those methods rely are ill-suited to determining whether any particular unauthorized transfer is protected by the doctrine of fair use.[210] Whereas the fair use analysis is subtle, contextual, and standards-based, software engines for filtering are rule-based, and the tnesion between the two persists even as the state of the art advances.[211] Filtering technology may thus never be equal to the task of separating infringing uses from fair ones, and the inevitable consequence of that failure will be blocking of lawful speech. Corporate copyright owners, who view traffic filtering and site blocking as preferred solutions, tend to discount the risk of over-blocking.[212] Judges and members of the public, however, are less blasé. In the policy debates over the Stop Online Piracy Act and the PROTECT IP Act, both of which required ISPs to block users' access to "foreign infringing sites," millions of Americans made it clear to Congress that protected speech should not be regarded as tolerable collateral damage in the war on piracy.[213] Across the Atlantic, the ECJ ruled in 2011 in *Scarlet v. SABAM* that a Belgian national court could not, as a matter of EU law, issue an injunction that would require an ISP to install and maintain a system for filtering P2P file transfers.[214] Such a system, the court said, would violate EU protections for freedom of information, because it could not be relied upon to distinguish adequately between lawful and unlawful file transfers.[215]

CAS does not entail any blocking or filtering of content, so the threat to freedom of expression associated with over-blocking is not an issue for broadband subscribers whose ISPs are parties to the MOU. In the CAS protocol, copyright owners identify files as infringing and report the alleged infringements to ISPs, but neither the copyright owner nor the ISP takes any action to block file transfers as they are occurring. To avoid issuing notices in response to *de*

---

[210] *See* Sonia K. Katyal & Jason M. Schultz, *The Unending Search for the Optimal Infringement Filter*, 112 COLUM. L. REV. SIDEBAR 83, 99-101 (2012) (arguing that automated filters are not equal to the task of identifying infringing works and assessing fair use).

[211] The critique of automated copyright enforcement first arose in debates in the late 1990s over digital rights management (DRM) software and statutory prohibitions on its circumvention. *See, e.g.,* James Grimmelmann, *Regulation by Software*, ____ YALE L. REV. ___ (200_); Edward W. Felten, *A Skeptical View of DRM and Fair Use*, COMM. ACM, Apr. 2003, at 57; Dan Burk & Julie Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41 (2001).

In more recent years, the same (still compelling) critique has been leveled against the use of filtering technology to block access to infringing content. *See* MEHAN JAYASURIYA, ET AL., PUBLIC KNOWLEDGE, FORCING THE NET THROUGH A SIEVE: WHY COPYRIGHT FILTERING IS NOT A VIABLE SOLUTION FOR U.S. ISPS (20__), available at http://www.publicknowledge.org/paper/pk-filtering-whitepaper.

[212] *See, e.g.,* IFPI DIGITAL MUSIC REPORT 22 (2012) (praising the South Korean government for requiring ISPs to block user access to websites, including P2P trackers). Much of the public relations material released by proponents of website blocking evades the issue of over-blocking and simply invokes the premise that infringing speech is not constitutionally protected. *See, e.g.,* REP. LAMAR SMITH, MYTH V. FACT: STOP ONLINE PIRACY ACT, available at http://judiciary.house.gov/issues/Rogue%20Websites/011812_SOPA%20Myth%20vs%20Fact.pdf (last visited June 25, 2012) (asserting without qualification that the website blocking provision in the Stop Online Piracy Act implicates no speech protected by the First Amendment).

[213] *See* Annemarie Bridy, *Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Prespective on ACTA, SOPA, and PIPA*, 30 CARDOZO ARTS & ENT. L.J. 153 (2012)

[214] Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), ECJ Case C-70/10 (2011), ¶¶ 52-54.

[215] *Id.* at ¶ 52.

minimis or protected uses of copyrighted works, copyright owners agree in the MOU to focus only on file transfers consisting of copyrighted works in complete or substantially complete form.[216] This is a commendable if blunt effort to accommodate fair use by treating transfers of partial copies as non-events.[217] On the whole, then, CAS should not be a major cause of concern for consumers when it comes to the protection of expressive freedoms, because content filtering is not a component of the protocol, partial copies are not noticed, and suspensions of Internet access are unlikely given the availability to ISPs of more palatable sanctions.

B. Privacy

Graduated response systems involve surveillance of Internet traffic for infringing file transfers, and they require ISPs to put names to the otherwise anonymous IP addresses associated with those transfers. Both of these features raise privacy concerns, and both have been found by the European Data Protection Supervisor to violate the EU Charter of Fundamental Rights and EU Data Protection and Privacy Directives.[218] Comparatively speaking, however, the legal climate for these activities in the United States is more hospitable than it is in the European Union. This is true for at least two reasons: First, the US government has not taken a coherent approach to privacy regulation in the digital environment, opting instead for a hodgepodge of sector-specific legislation and permissive industry norms for online monitoring and data collection.[219] Second, corporate copyright owners have been very successful in convincing courts and legislators that the right to go incognito online should not shield alleged infringers from liability.[220]

1. Surveillance

Research DPI

Surveillance for copyright enforcement is at its most invasive when it is hardwired within an ISP's network. ISPs can install dedicated devices that use DPI to detect and block file transfers identified as (or as likely to be) infringing.[221] Blocking can be done crudely on a

---

[216] MOU, *supra* note 12, at 6.

[217] The amount of the copyrighted work borrowed and the extent to which the borrowing creates a market substitute for the copyrighted work are factors in the fair use analysis, which means that complete or substantially complete copies of copyrighted works are much more likely than partial copies to be infringing. *See* 17 U.S.C. § 107 (setting forth the fair use factors).

[218] *See supra* note 64 and accompanying text. The finding, however, has not caused France to alter the Hadopi protocol, nor has it had any impact on the Irish High Court's analysis of privacy issues relating to Eircom's protocol in Ireland.

[219] *See generally* Chris Jay Hoofnagle, NEW CHALLENGES TO DATA PROTECTION STUDY - COUNTRY REPORT: UNITED STATES, European Commission Directorate-General Justice, Freedom and Security Report (2010). It should not surprise us that privacy policy is in disarray, because, as Daniel Solove has observed, privacy as a concept is also in disarray. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008).

[220] *See, e.g.,* Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004) (denying a motion to quash plaintiff's subpoena to Cablevision demanding the identities of defendants, alleged P2P infringers, based on their IP addresses); 17 U.S.C. § 512(h) (2012) (providing that copyright owners may obtain and serve subpoenas on ISPs to identify subscribers who allegedly infringe copyrights by uploading files to servers maintained by the ISPs.)

[221] One example of such a device is AudibleMagic's CopySense appliance, which is marketed widely to colleges and universities for use in managing P2P file sharing on their networks. Audible Magic, Technology Overview, http://audiblemagic.com/technology.php (last visited July 9, 2012). Another is Blue Coat's PacketShaper, an enterprise appliance for which marketing materials boast "the x-ray vision needed to monitor today's network traffic." Blue Coat, PacketShaper, https://www.bluecoat.com/products/packetshaper (last visited July 9, 2012).

protocol-specific basis, e.g., blocking all BitTorrent traffic, or more granularly by matching digital fingerprints, file hashes, or other unique identifiers associated with transiting files against a database maintained by the ISP or a third party provider.[222] ISP-based surveillance requires that all traffic for all customers be scrutinized all the time, creating an environment of pervasive and invisible surveillance. James Boyle described this phenomenon in 1997, citing Michel Foucault's work on sovereign power and penal systems, as the "privatization of the Panopticon."[223] More recently, Derek Bambauer cast it in Orwellian terms.[224] When Boyle was writing, the architecture was willing, but the technology was weak. Whereas ISPs have always controlled the point on the network through which every bit of information a user sends and receives must pass, they have not always enjoyed the ability to probe, mine, and sort that information for a dozen different ends—including copyright enforcement.[225] They do now, though, thanks to DPI.

Privacy scholars have questioned whether ISPs' use of DPI violates the Wiretap Act.[226] Despite its questionable legality, however, DPI has become standard operating procedure for ISPs for such purposes as congestion management and spam- and virus-filtering.[227] Although the technology has been adopted by several colleges and universities in an effort to curb illegal file sharing on campus networks, major ISPs have not warmed to the idea of using DPI for copyright enforcement.[228] The fact that DPI can be quite easily defeated by encryption has not helped copyright owners make the case for it to ISPs, which also have other reasons to be reluctant.[229] The Federal Communications Commission (FCC) sanctioned Comcast in 2008 for its use of DPI

---

[222] *See* Klaus Mochalski et al., *Copyright Protection in the Internet*, Ipoque (2009), http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-copyright-protection-internet.pdf (explaining different mechanisms for blocking and filtering infringing traffic, including ones that operate at the host or application level—e.g., DNS blocking, protocol blacklisting, port blocking—and ones that operate at the file level—e.g., fingerprinting, hash-based identification, and watermarking).

[223] James Boyle, *Foucault in Cyberpsace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 197, 198 (1997).

[224] Derek Bambauer, *Orwell's Armchair: Filtering on the March*, __ CHI. L. REV. __ (2012).

[225] *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (2009) (discussing the unique position ISPs occupy in the economy of Internet surveillance).

[226] Paul Ohm concludes that the use of DPI, particularly by the backbone providers that serve ISPs rather than retail customers, most likely violates the Wiretap Act. *Id.* at 1486. He discusses the possibility that retail ISPs could be covered by the consent exception to the ECPA, based on their terms of service, but he points out that applicable state wiretapping laws might require two-party consent, which cannot be secured through terms of service that bind only one of the parties to any given online communication. *Id.*

[227] Sandvine, a Canadian provider of DPI hardware to ISPs worldwide, reported in 2009 that 90% of its 160 customers were using the technology to manage traffic on their networks. *See* Nate Anderson, *DPI Vendor Says 90% of ISP Customers Engage in Traffic Discrimination*, ARS TECHNICA, Aug. 3, 2009, http://arstechnica.com/tech-policy/news/2009/08/network-neutrality-dead-in-practice-as-most-isps-throttle.ars.

[228] *See* Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at 84, 123 (discussing the use of DPI in higher education IT network management); Milton Mueller et al., *Policing the Network: Using DPI for Copyright Enforcement*, 9 SURVEILLANCE & SOC'Y 348, 361 (2012) (stating that although ISPs have varied in the intensity of their opposition to using DPI for copyright enforcement, there is no evidence that any has actively embraced or advocated it).

[229] *See* Rob Frieden, *Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 633, 645 (2008) (asserting that ISPs' use of DPI raises questions about their continued eligibility for safe harbor under section 512 of the DMCA); Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, *supra* note 11, at 120-124 (discussing a 2009 district court case holding that a Usenet host engaged in active network management is not entitled to invoke copyright law's protections for "mere conduits").

to manage congestion by blocking BitTorrent P2P transfers, but the sanction was later invalidated in a decision by the Court of Appeals for the D.C. Circuit, which held that the FCC lacked statutory authority to impose the sanction.[230] Net neutrality regulations promulgated by the FCC following the Comcast sanction, and currently under review in the D.C. Circuit, do not prohibit ISPs from intervening at the network level to enforce copyrights, so long as the efforts undertaken are reasonable.[231] Although those regulations will likely not survive judicial review, the exception they make for copyright enforcement highlights the extent to which the US government has sought to clear the way for increased ISP cooperation with copyright owners and the extent to which copyright concerns have fully infiltrated the debate over net neutrality.

A less intrusive and more common type of surveillance associated with graduated response is one in which copyright owners hire third party agents to monitor public P2P file sharing networks by joining them and documenting IP addresses that appear to be sharing infringing files.[232] ISPs play no role in this type of self-help monitoring, which is sometimes referred to as "over-the-top" (OTT) surveillance because it operates at the Internet's application layer and not at the level of physical infrastructure.[233] The field of OTT surveillance is limited to publicly accessible P2P networks, and the monitors can be detected and avoided based on their behavior—albeit not by the average user.[234] OTT surveillance provides the evidentiary basis for sanctions in the French and Irish implementations of graduated response, and corporate rights owners in the US have relied on it since the early 2000s, when they began monitoring P2P networks in conjunction with their litigation campaign against individual file sharers.[235] Given the publicity surrounding that campaign, informed users of public P2P networks know by now that they are not sharing files in an unmonitored environment.[236]

[230] Comcast Corp. v. Fed. Commc'ns Comm'n, 600 F.3d 642 (2010). Comcast was not using DPI for copyright enforcement purposes.

[231] *See* 47 C.F.R. § 8.9 (2012) ("Nothing in this part prohibits reasonable efforts by a provider of broadband Internet access service to address copyright infringement or other unlawful activity."); Verizon v. Fed. Commc'ns Comm'n, No. 11-1355 (D.C. Cir. 2011) (seeking to invalidate net neutrality rules issued by the FCC in 2010).

[232] DtecNet is probably the largest provider in this space, but other firms, such as Peer Media Technologies, also offer P2P monitoring services. *See* DtecNet, Company History, http://dtecnet.com/EN/About/Company%20History.aspx (last visited July 3, 2012) (stating that the company operates in more than 25 countries); Peer Media Technologies, Notification Services, http://peermediatech.com/notification.html (last visited July 3, 2012) (describing P2P and cyberlocker monitoring services).

[233] *See* Mueller et al., *supra* note 224, at 361 (using the term). By way of further explanation, P2P networks are classified as "overlay networks" because they run at the application layer, on top of the underlying physical structure of the Internet. *See* Enrico Marocco et al., *Peer-to-Peer Infrastructure: A Survey of Research on the Application-Layer Traffic Optimization Problem and the Need for Layer Cooperation*, 47 IEEE COMMC'NS MAGAZINE 107 (2009).

[234] *See, e.g.*, Anirban Banerjee et al., *The P2P War: Someone Is Monitoring Your Activities!*, 52 J. COMPUTER NETWORKS 1272 (2008) (explaining how to identify and avoid the "fake users" employed by the RIAA and the MPAA on P2P networks).

[235] *See* Annemarie Bridy, *Why Pirates (Still) Won't Behave: Regulating P2P in the Decade after Napster*, 40 RUTGERS L. J. 565, 590-596 (discussing the surveillance program on which the RIAA's litigation campaign relied to produce evidence of P2P infringements).

[236] *See, e.g.*, RIAA, About Copyright Notices, https://www.riaa.com/toolsforparents.php?content_selector=resources-music-copyright-notices (last visited July 10, 2012) (emphasizing that P2P file sharers are not anonymous).

Under the MOU, copyright owners take the OTT approach to monitoring, which is significantly less invasive of user privacy than DPI-based surveillance. While Trisha Meyer and Leo Van Audenhove have argued rightly that graduated response contributes to the normalization of surveillance on the Internet,[237] not all methods of online surveillance are equally intrusive, and they should not be treated as such. Not only is the field of surveillance much narrower in OTT monitoring, the activity in question takes place in plain view of anyone who cares to join the network.[238] Publicly accessible P2P networks operate by making the contents of every connected storage device searchable and accessible to other devices on the network. No participant can reasonably expect the contents of his or her hard drive to remain private when he or she is broadcasting (and offering to share) them on the open Internet.[239] Users who want to engage in unmonitored P2P transactions can do so via password-secured networks or virtual private networks (VPNs), and there is actually some evidence that OTT monitoring by copyright owners has driven a percentage of P2P traffic underground.[240] If copyright owners were to attempt to monitor online activity in such secured environments, the privacy implications would be more real. But given the open nature of the networks in question, copyright owners are not breaching the privacy of participants by capturing the IP addresses associated with potentially infringing file transfers.[241] Smart people encrypt

One privacy impact of CAS that follows from OTT surveillance is ISP retention and reporting of information about the alleged infringements of subscribers. Under the MOU, ISPs track and report the notices they receive and the alerts they send to every subscriber, even after the CAS protocol has run its course for subscribers who are repeat recipients.[242] ISPs send this information monthly in anonymized form to copyright owners, who may use it in litigation to seek subpoenas to identify subscribers and to support claims of infringement.[243] Such information is not retained forever, though. Retention is limited by the "reset" provision in the MOU, which permits ISPs to expunge all prior notices and alerts from a subscriber's account if the subscriber goes 12 months without receiving an additional alert.[244] To assure protection of consumer privacy, expungement on reset should be mandatory rather than permissive.

wait - it anonymized how can do subpoena?

this should be cleared up

[237] Trisha Meyer & Leo Van Audenhove, *Surveillance and Regulating Code: An Analysis of Graduated Response in France*, 9 SURVEILLANCE & SOC'Y 365, 375 (2012).

[238] As the Irish High Court noted in *EMI v. UPC*, "DtecNet does what any user of a peer-to-peer network does in order to obtain a download. No extra information is obtained." EMI v. UPC, [2010] IEHC 377, ¶ 34.

[239] In one study, 100% of peers participating in observed P2P networks over a 90-day period between January and March 2006 made contact with one or more fake users. Banerjee et al., *supra* note 230, at 1272.

[240] TorrentFreak, a site dedicated to P2P file sharing, recently rated VPN providers based on the degree to which they protect user anonymity in the face of third party requests for identifying information.

[241] The Irish High Court reached the same conclusion when it invalidated the Data Protection Commissioner's cease and desist order against Eircom. *See EMI Records*, [2012] IEHC at ¶ 7.2 (describing participation in a BitTorrent swarm as "an open communication with all comers on the [I]nternet" and concluding that monitoring of such activity cannot be fairly equated with wiretapping).

[242] MOU at 13 (providing that the ISP may stop sending alerts after the sixth one but must "continue to track and report the number of ISP Notices the Participating ISP receives for that Subscriber's account, so that information is available to a Content Owner Representative if it elects to initiate a copyright infringement action against that Subscriber").

[243] MOU at 15 ("[T]he Content Owner Representatives…may use such reports or data as the basis for seeking a Subscriber's identity through a subpoena or order or other lawful process.").

[244] MOU at 13

2. Loss of Anonymity

Knowing the IP address of a file sharer, which copyright owners can by means of OTT monitoring, is not the same as knowing the identity of the person who owns the account to which that IP address corresponds. Matching a publicly visible IP address to the not-publicly-visible identity of a particular account holder raises a distinct privacy concern, albeit one with which US courts have already grappled in the context of online file sharing. Such cases have consistently held that a person's right to anonymity is outweighed by a copyright owner's interest in good faith enforcement.[245] Case law developed during the RIAA's now-abandoned campaign of litigation against individual file sharers permits copyright owners to obtain the identities of alleged P2P infringers by naming them as John Doe defendants in lawsuits and then issuing subpoenas to their ISPs.[246] The match can thus be made by the ISP and disclosed to the complaining copyright owner, albeit not outside litigation and the due process that it affords.[247]

With respect to the preservation of anonymity, the notice system at the core of graduated response does not require disclosure of subscriber identifying information to copyright owners. This is a significant virtue of the model, which interposes the ISP between the subscriber and the copyright owner, thereby shielding the subscriber's identity. Non-disclosure is the rule in the French and Irish implementations described in Part II above, and it is also the rule in CAS, with one exception: An ISP is required under CAS to disclose the identity of a subscriber who raises the defense of authorization in an independent review proceeding, if such disclosure is necessary for the copyright owner to assess the validity of the defense.[248] The exception is narrowly defined and leaves it to the reviewer rather than the copyright owner to decide whether disclosure is necessary in a given case.

All in all, CAS should not be especially worrisome for broadband subscribers with respect to privacy. It does involve surveillance of online activity, but the monitoring it incorporates is publicized for deterrence purposes, limited to open P2P networks, and carried out horizontally by peers rather than vertically by all-seeing intermediaries. OTT monitoring is much less comprehensive and surreptitious than ISP-based surveillance, which would be a truly

---

[245] *See, e.g.,* Virgin Records Am., Inc. v. Doe, No. 5:08-CV-389-D, 2009 U.S. Dist. LEXIS 21701 (E.D.N.C. Mar. 16, 2009) (denying defendant's motion to quash plaintiff's subpoena to defendant's ISP on the ground that the First Amendment protects anonymous speech but not anonymous copyright infringing speech).

[246] *See, e.g.,* UMG Recordings, Inc. v. Does, 64 Fed. R. Serv. 3d (Callaghan) 305 (N.D. Cal. 2006) (granting the plaintiff copyright owner's motion for expedited discovery in the form of a Rule 45 subpoena requiring an ISP to identify an alleged infringer).

[247] The DMCA provides a more streamlined procedure for identifying alleged infringers when the infringement results from a user's unauthorized storage of copyrighted material on the server of a web site operator or ISP. *See* 17 U.S.C. § 512(h) (setting forth procedures for a copyright owner to follow to obtain a pre-litigation subpoena to identify an alleged infringer). That streamlined procedure, which does not require filing a lawsuit, has been held by courts not to apply in cases involving P2P file sharing, for which the technology did not exist when the DMCA was enacted. *See* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

[248] *See* MOU, *supra* note 12, at 14 ("The Independent Review Program shall allow for the Subscriber to remain anonymous to the Content Owner Representatives…except in cases where the Subscriber elects a defense in which the Subscriber's identity will be disclosed."), 32 (providing for disclosure of the Subscriber's identity in a case involving the defense of authorization "unless the Reviewer concludes that the Copyright Owner does not need to know the identity of the Subscriber to evaluate the Subscriber's claim that his or her activity was authorized").

objectionable development in the evolution of online copyright enforcement. Moreover, CAS does not require disclosure of subscriber identities to copyright owners, except in very limited circumstances. In that respect, CAS is more protective of privacy than is mass John Doe litigation, the more cumbersome enforcement model that it supplants.[249] Finally, CAS does involve retention and reporting of information about the alleged infringements of individual subscribers, but the "reset" function in the protocol serves as an important check on the size of that data pool.

C. Fairness

Concerns about procedural and substantive fairness in graduated response protocols are front and center in the growing body of academic literature on this subject.[250] In France, such concerns led the Constitutional Council to reject the Hadopi legislation in its initial form and to require judicial review of all disconnection decisions.[251] Because the MOU sets the goal of automating the individual components of CAS to the maximum extent practicable, the design of the system must be closely scrutinized to ensure that fairness does not fall victim to efficiency. This section focuses on four specific elements of fairness: presumption of innocence; opportunity for neutral adjudication; predictable application of established legal standards; and availability of defenses.

1. Presumption of Innocence

In civil suits for copyright infringement, the burden of proof is on the plaintiff, who must prove both ownership of a valid copyright and infringement of an exclusive right granted by section 106 of the Copyright Act.[252] CAS alters this allocation of burdens by making it the responsibility of the accused (i.e., the recipient of a fifth or sixth copyright alert) to raise and prove a defense to infringement in order to avoid a sanction. In addition to shifting the burden of proof with respect to infringement, the MOU creates a presumption of accuracy in favor of the copyright owner, as discussed above in Part III.B above, with respect to both the capture of IP addresses and the identification of copyrighted content. The presumptions of accuracy attach under the MOU as long as the copyright owners' methods of collection and identification have not been found "fundamentally unreliable" by a technical expert. On the strength of these presumptions, notices from the complaining copyright owner are treated as proof of infringement sufficient to trigger the imposition of a sanction. Such treatment was criticized in *Corbis Corp. v. Amazon.com*, a case interpreting the repeat infringer provision of the DMCA.[253]

---

[249] *See* Bridy, *Is Online Copyright Enforcement Scalable?*, *supra* note 3, at 719-725 (arguing that John Doe litigation is a "dysfunctional workaround" for the DMCA's failure to scale for P2P file sharing).

[250] *See id.* at 736 (asserting that graduated response systems must be designed to honor the competing values of efficiency and fairness); Nicolas Suzor & Brian Fitzgerald, *The Legitimacy of Graduated Response Schemes in Copyright Law*, 34 UNIV. OF NEW S. WALES L.J. 1, 24 (2011) (asserting that certain minimum standards of due process must be upheld in implementations of graduated response); Yu, *The Graduated Response*, *supra* note 18, at 1419 (2010) (arguing that a graduated response system must respect the rule of law and the norms of fairness and legitimacy); LaFrance, *supra* note 136, at 175 (finding that CAS "comes up short in several respects" when viewed through the lens of fairness).

[251] *See* note 76 *supra* and accompanying text.

[252] A&M Records v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001).

[253] *See* Corbis Corp. v. Amazon.com, 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004) (stating that notices from a copyright owner can bring a potential infringement to a provider's attention but are not in themselves

The allocation of burdens built into CAS is troubling because it conflicts with a basic principle underlying our justice system—that a person accused of having engaged in illegal conduct is presumed innocent proven liable in a court of law. In keeping with that principle, Peter Yu has called for a focus in graduated response on *proven* infringers as opposed to *alleged* infringers.[254] As I have argued elsewhere, however, litigation doesn't scale well for enforcing copyrights against P2P file sharers.[255] Graduated response is effective as an enforcement strategy only if it can function most of the time as a litigation substitute, and not as a litigation supplement. That having been said, the MOU does more than it should to ease evidentiary burdens on copyright owners. In addition to relieving them of the customary burden of having to prove their allegations before a sanction is imposed, it affords them rebuttable presumptions of evidentiary accuracy as long as their technical methods are not "fundamentally unreliable."[256] Allocating the burden of proof on infringement to the accused is a significant compromise of fair process. Adding to that compromise the presumption that the evidence offered against the accused is valid unless it was collected in a grossly negligent way is a bridge too far. Given that CAS treats accumulated notices of infringement as sufficient evidence to justify a sanction (or to require the accused to prove a defense in order to avoid the sanction), the methods of address collection and content identification that underlie notices of infringement should be held to a much higher technical standard. Copyright owners should be required by the MOU to adopt technical means of collecting IP addresses and identifying content that are affirmatively and demonstrably reliable. Moreover, the accuracy of those methods should be verifiable by independent experts who do not work as consultants for CCI and who are not bound by nondisclosure agreements.

2. Opportunity for Neutral Adjudication

Another aspect of procedural fairness is the opportunity to be heard by a neutral third party before any deprivation of rights or property occurs. As discussed above, CAS diverges from litigation procedure by presuming the accuracy of the allegations contained in copyright alerts and shifting the burden onto the recipient to show that s/he is not a repeat infringer. While CAS does not provide a hearing on the merits of each alert before it is issued, it does provide an independent review procedure, as described in Part III.B.2, for any subscriber who wants to contest the accuracy or validity of one or more alerts after the fact. The imposition of a mitigation measure is staid pending the outcome of review.[257] The timing of the opportunity to contest allegations under CAS is later than optimal, but the fact that the opportunity comes before any sanction is imposed preserves an important element of fairness.

The review focuses entirely on a spare written record—the "standard package"—documenting both the alleged infringements and the subscriber's assertion of one or more

---

evidence of infringement, because they could be erroneous). *But see* Perfect 10 v. CCBill LLC, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004) (concluding that a provider who receives repeat notices of infringement from a copyright owner but does not terminate the account of the subscriber in question has not reasonably implemented a repeat infringer policy for purposes of the DMCA).

[254] Yu, *The Graduated Response*, *supra* note 18, at 1418 (emphasis in original).

[255] Bridy, *Is Online Copyright Enforcement Scalable?*, *supra* note 3, at 719-725.

[256] MOU, *supra* note 12, at 27, 28.

[257] *Id.* at 30.

defenses, along with supporting facts.[258] In keeping with the efficiency imperative, there are no hearings, and there is no discovery.[259] The austerity of that rule is tempered, however, by the provision in the MOU that enables the reviewer to seek additional information, if needed, from one or more of the parties.[260] And the subscriber's right to elect a traditional judicial forum, where hearings and discovery are the rule, is not foreclosed.[261]

As far as the neutrality of the reviewers is concerned, CAS improves on the Eircom model by requiring third party adjudication, but it does not go as far as Hadopi, which requires a court order for the imposition of a sanction. The reviewers who decide CAS subscriber appeals are structurally independent, having no employment relationship with copyright owners, ISPs, or CCI. Such independence enables but does not guarantee their impartiality.[262] As with any arbitral scheme arising from a mass contract of adhesion, there is in CAS the potential for anti-consumer bias associated with the repeat player effect.[263] The reviewers work for AAA, which works for CCI, which at the end of the day is an entity formed for the benefit of copyright owners. Again, though, participation in the independent review program created by the MOU is not mandatory; subscribers accused of infringement remain free to challenge the allegations against them in court, presumably through an action for declaratory judgment of non-infringement. The subscriber's ability to opt out distinguishes the independent review program—for the better—from the mandatory arbitration schemes to which a wide range of consumer disputes arising under mass contracts are now subject in the United States.[264] Weighing the expense of litigation and the attendant risk of statutory damages against the moderate sanctions outlined in the MOU, very few subscribers are likely to choose litigation.[265] Notwithstanding that fact, preserving the option of litigation allows subscribers to get full procedural due process if they want it.

Good to have a choice

3. Predictable Application of Established Legal Standards

Procedural fairness is of course only part of the equation when it comes to the fair resolution of disputes. Substantive fairness is also required. Under the MOU, the substantive legal rules to be applied in independent review proceedings come from "prevailing legal

---

[258] *Id.* at 31 (specifying the contents of the Application to Commence Independent Review (ACIR) package)

[259] MOU, *supra* note 12, at 33.

[260] *Id.* at 32.

[261] *See id.* at 26 (stating that the independent review process is "just one avenue of appeal" and that it "does not prevent [the parties] from addressing [their] disputes through the courts").

[262] *Cf.* Alan Scott Rau, *Integrity in Private Judging*, 38 S. TEX. L. REV. 485 (1997) (analyzing structural factors that tend to undermine impartiality in private arbitrations).

[263] *See id.* at 524 (asserting that an arbitrator's incentive to secure future business from a repeat customer is corrosive of impartiality). Mary LaFrance has questioned whether the CAS independent review process will inevitably suffer from the problem of "embedded neutrals." LaFrance, *supra* note 136, at 183 (citing a study by Nancy Welsh on bias in arbitration).

[264] *Cf.* Carter Dougherty, *Consumers May See New Limits on Mandatory Arbitration*, BLOOMBERG.COM, May 21, 2012, http://www.bloomberg.com/news/2012-05-21/consumers-may-see-new-limits-on-mandatory-arbitration.html (reporting on the ubiquity of mandatory arbitration provisions in contracts for consumer financial services).

[265] As John M. Owen points out, the remedies available under CAS are less harsh than the remedies available at law. John M. Owen, *Graduated Response and the Market for Copyrighted Works*, 27 BERKELEY TECH. L.J. 559, 608 (2012).

principles as determined by United States federal courts"[266] and interpreted by the AAA-commissioned, CCI-board-approved independent expert.[267] As of this writing, that expert has not been publicly identified, so it is impossible to assess his or her independence and credentials. Whoever is chosen, however, is required by the MOU to receive input from the copyright owner representatives concerning *their* interpretation of "prevailing legal principles."[268] This mandate raises doubts about the extent to which the expert's independence will be respected and sustained.

The prospect that the expert will be captured is a real one, particularly in light of the fact that there is no provision in the MOU for public disclosure of the outline of applicable legal principles the expert is required to prepare and maintain.[269] When potentially biased interpretations of the law govern an arbitral process potentially subject to repeat player bias, there is little reason to believe that outcomes will be substantively fair. The RIAA has put forward some demonstrably unsound interpretations of copyright law over the years. Its web site states, for example, that "making unauthorized copies of copyrighted music recordings is against the law" and that "many peer-to-peer (P2P) programs" have been held by courts to "inherently amount to copyright infringement and therefore constitute a crime."[270] Anyone who understands the complexities of fair use, the law concerning dual-use copying technologies, and the difference between civil and criminal infringement knows that those are far from accurate statements of "prevailing legal principles."[271] If such statements are emblematic of the legal principles that will govern appeals under CAS, then CAS can have no credible claim to legitimacy and impartiality.

Compounding the problems of potential expert capture and opaque rules of decision, no written opinions will issue from the independent review process, which means there is really no way for any member of the public to determine whether the rules, whatever they are, are being applied consistently across cases.[272] The system's lack of transparency, which will be discussed at greater length below in Part IV.E, undermines substantive fairness. To address the transparency issues related to adjudication under CAS, CCI should disclose the identity of the AAA-commissioned independent expert, so that members of the public can assess his or her independence and credentials. CCI should also disclose the substantive rules that will be applied

---

[266] MOU, *supra* note 12, at 35.

[267] *Id.*

[268] *See id.* (providing that parties to the MOU must be given a means to "provide input [on material questions of law]....so as to ensure that the expert's determinations are fully-informed and reflect prevailing laws as determined by United States federal courts").

[269] *See id.* at 35 (requiring the copyright expert "to outline [and update from time to time] prevailing legal principles of fair use...and any other legal principles necessary for resolution of issues within the scope of the Independent Review process").

[270] RIAA, The Law, https://www.riaa.com/physicalpiracy.php?content_selector=piracy_online_the_law (last visited August 1, 2012).

[271] Operators of P2P file sharing services such as Napster, Grokster, and LimeWire have been found civilly liable for the copyright infringements of their users, but there has never been a legal decision that P2P software is inherently unlawful or that the use of such software necessarily constitutes an infringement, let alone a criminal one.

[272] *See* MOU, *supra* note 12, at 34 ("Reviewers shall not prepare written decisions in the cases they decide."). If, however, a subscriber who raises a defense does not prevail, the MOU requires the reviewer to prepare a "short description of the rationale for the denial." *Id.* at 33. The rationale is disclosed to the subscriber but not to the public. *Id.*

by AAA independent reviewers. While it would be ideal for written decisions to be recorded and published to ensure consistency across time and cases, such a practice would likely detract more from efficiency than it would add to fairness. The public needs to know, however, whether the independent reviewer's rules of decision come from copyright law or from the RIAA, because they are apparently not the same rules.

4. Availability of Defenses

The Copyright Act provides a range of defenses and exceptions to copyright infringement. While the exclusive rights of copyright owners are fully enumerated in just two sections of code, section 106 and section 106A, the following fifteen sections—107 through 122—enumerate a wide range of limitations and exceptions that are crucial for maintaining a balanced copyright system.[273] CAS, by contrast, permits a subscriber to raise only six defenses, and only two of those—fair use and publication before 1923—are grounded directly in copyright law.

Why did they skip some?

It is true that many of the defenses and exceptions provided in the Copyright Act are not relevant to the lion's share of infringement claims arising from P2P file sharing. But CAS, on principle, should permit a subscriber to raise *any* relevant defense that is cognizable under the public law of copyrights. There are, for example, several reasons for which a work can be in the public domain that are unrelated to publication before 1923, which is the only out-of-copyright scenario the MOU contemplates. Works in the public domain include those published between 1923 and 1963 whose copyrights were not renewed, works published before 1989 without proper copyright notices, and most works created by the U.S. government.[274] The rules concerning lapse and loss of protection are complicated, even byzantine, but they are nevertheless the rules. If the substantive law of the independent review under CAS is U.S. copyright law, as it should be, then all relevant provisions of U.S. copyright law should be the law of CAS.[275]

This must just be an oversight

To summarize, when it comes to the norm of fairness CAS leaves much to be desired. With respect to procedural fairness, the system lacks the presumption of innocence, although it does allow for an appeal to a third party neutral before any sanction imposed. The third party neutral is structurally independent but nevertheless subject to the potential biases associated with mass consumer arbitration. The saving fact for procedural fairness under CAS is that subscribers are not asked to waive their right to relief through the courts. Regarding substantive fairness, CCI's failure to disclose the rules that will govern appeals makes it impossible for the public to know whether those rules adequately capture the nuances of copyright law and accurately reflect existing case law. Finally, the defenses available to subscribers are unduly limited and fail to align completely with copyright law.

---

[273] 17 U.S.C. §§ 106-122 (2012).

[274] *See* Pamela Samuelson, *Reforming Copyright Is Possible*, CHRONICLE OF HIGHER ED., July 9, 2012 (listing the various ways that works can fall into the public domain).

[275] Mary LaFrance has also criticized CAS for placing limits on available defenses. LaFrance, *supra* note 136, at 176-177.

D. Proportionality

The principle of proportionality, a close cousin of substantive fairness, is expressly incorporated into the EU Copyright Directive, which provides that sanctions and remedies for copyright infringement should be "effective, proportionate and dissuasive."[276] When the ECJ analyzes legislation to determine whether it conforms with the principle of proportionality, it considers three factors: (1) whether the law in question is necessary to accomplish its articulated goal, (2) whether the law is suitable in terms of the relationship it establishes between ends and means, and (3) whether it imposes an excessive burden on the individual at whose conduct it is directed.[277] Three strikes protocols that culminate in disconnection have been found by the EU Data Protection Supervisor to violate the principle of proportionality,[278] although the Irish High Court reached the opposite conclusion in the Eircom case.[279]

As a form of private legislation, the MOU invites analysis of the proportionality of the sanctions it incorporates. The proportionality assessment for CAS is markedly different than for either Hadopi or Eircom, however, because CAS doubles the number of strikes that precede a sanction, and CAS is unlikely to entail suspension of access. In these important respects, CAS is less draconian than its European counterparts, and its moderation makes for a better fit between the wrong and the remedy. This question of fit is at the core of the proportionality analysis. As the brief analysis below will demonstrate, CAS is proportionate as an approach to combating P2P infringement.

1. Necessity

The stated goals of CAS are education and deterrence. Privately administered graduated response protocols represent one way, but by no means the only way, to achieve those twin goals. The argument for the necessity of graduated response as a deterrent is based on mounting empirical evidence that other means haven't worked. Mass litigation against end users had only limited deterrent effects.[280] And the various provisions of the DMCA that were intended to control online infringement—the repeat infringer, notice-and-takedown, and pre-litigation subpoena provisions—all proved inapplicable to the P2P distribution scenario.[281] As the limits of public law for fighting P2P infringement have been revealed, the case for turning to privately administered graduated response as an alternative model of enforcement has become stronger. There is no doubt that supply-side interventions continue to be necessary in the form of increased offerings of lawful content to consumers at reasonable prices across delivery platforms. It would be unfair, however, to foreclose new models of enforcement when existing ones have fallen short and the problem remains a serious one. Graduated response is not strictly necessary for enforcing

---

[276] Directive 2001/29/EC, art. 8, 2001 O.J. (L 167) 18 (EC).

[277] *See* Tor-Inge Harbo, *The Function of the Proportionality Principle in EU Law*, 16 EURO. L.J. 158, 165 (2010).

[278] Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010 O.J. (C 147) 5.

[279] *See supra* note 121 [citing EMI Records].

[280] *See* Bridy, *Why Pirates (Still) Won't Behave: Regulating P2P in the Decade after Napster*, *supra* note 234, at 604 (citing a study by the Pew Internet Project).

[281] *See* Bridy, *Is Online Copyright Enforcement Scalable?*, *supra* note 3, at 716-725.

copyrights online, but a properly calibrated system of privately administered warnings and sanctions is reasonable to try in light of past failures.

2. Suitability

As a means to achieving the ends of education and deterrence, the notice and sanction framework in CAS satisfies the test of suitability. With respect to education, copyright alerts containing escalating rhetoric under CAS provide information to users about copyright law and the sanctions for violating it. After receiving two notices, users must personally acknowledge having read and assimilated that information. In addition, one of the sanctions contemplated under the MOU is diversion to a web site requiring some form of interactive copyright education. It is absolutely vital, of course, that the information about copyright law disseminated through CAS be both accurate and complete. The dissemination of misinformation about copyrights would make CAS a damaging and unsuitable educational tool.

With respect to deterrence, the preliminary evidence from Hadopi and Eircom is that very few users who receive a first notice of infringement receive any subsequent notices. This suggests that the receipt of notices in the context of a graduated response system has a meaningful deterrent effect on infringers. It will be important for CCI to monitor and disclose whether CAS has similar deterrent effects. If evidence gathered over time shows that it doesn't, then the protocol should be suspended as unsuitable.

3. Burden on Individual Rights

The third and final element to consider in assessing proportionality is the extent to which CAS burdens the rights of individuals in order to achieve its goals. Because CAS contemplates a range of possible sanctions, and it is not clear *ex ante* which ones ISPs will choose, this part of the analysis will vary depending on each ISP's implementation. In general, the greater a sanction's impact on a user's ability to access lawful content and applications, the greater the burden it imposes, and the less the likelihood that it can be justified in the name of enforcing copyrights. Sanctions affecting speed and service tier, which are likely to be the most stringent sanctions imposed under CAS, are ~~much less burdensome than an~~ outright suspension of access. It bears noting in this context that the sanctions listed in the MOU, which target individual users only, are exponentially less burdensome to users collectively than a proposed sanction like DNS blocking, which makes entire web domains unavailable to all users everywhere.[282] Given a choice between an enforcement regime that targets individuals and one that targets domains, the one that targets individuals will ultimately burden many fewer users and much less expression.

E. Transparency

Of the five norms on which this Article focuses, transparency is the one the MOU honors least. The lack is evident in three discrete domains related to CAS—design, oversight of implementation, and outcomes. Across these domains, an endemic lack of disclosure undermines the credibility of the system and the public's confidence in it.

[282] The controversial—and ultimately abandoned—Stop Online Piracy Act contained a provision requiring ISPs to block access to "rogue sites" by disrupting the addressing system by means of which an Internet domain name resolves to its corresponding IP address. *See* Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011).

1. Design

The MOU is *formally* private law, and the private law that corporations make amongst themselves is generally not subject to public input. The MOU is *functionally* public law, however, insofar as it requires specific and substantial changes to the terms of service that bind millions of broadband subscribers.[283] Moreover, the government's overt blessing gives the enterprise the whiff of public law and raises further questions about the closeted nature of the undertaking. Comparatively speaking, the process from which CAS emerged looks more like the deal-making process that produced the Eircom/IRMA settlement than like the policy-making process that produced Hadopi. That's too bad. The secrecy surrounding the MOU's negotiation compromises the legitimacy of CAS and justifies Mary LaFrance's description of the agreement as "a 'black box' industry compact."[284]

As law that is formally private but functionally public, the MOU should not have been negotiated entirely out of the public's view and without any input from public interest groups. One wonders in this regard about the timing of the advisory board appointments and why they weren't made *before* the details of the agreement were hammered out. From the point of view of transparency, it is commendable that the MOU itself has been made public and is available for download from CCI's website. It would have been much better, though, if the document had not been introduced to the public and presented to the CCI advisory board as a done deal.

2. Implementation

The parties to the MOU have made some meaningful gestures toward openness with respect to the implementation and oversight of CAS: they published the MOU in its entirety, created a public web site for CCI, and publicly identified the members of both the CCI executive committee and its advisory board. These gestures do not go far enough, however, when so much other vital information about the system and its operation remains closely held. Of particular concern is the secrecy surrounding both the technology underlying CAS and the rules that will be applied in the independent review program.

CCI has released no information about the technology underlying CAS or the identity of the independent technical expert hired to evaluate that technology. Moreover, the MOU prohibits the independent expert from disclosing any findings of technical inadequacy to third parties without the express written consent of the relevant parties to the MOU. If a finding of inadequacy goes unremedied, the expert is not permitted to disclose that fact without written permission—not even to the CCI advisory board. The secrecy to which the independent technical expert is bound is a genuine cause for concern in light of the fact that a copyright owner can decline to adopt expert recommendations without breaching the MOU[285] and can continue to send notices of infringement generated by systems that are unreliable, as long as they are not "fundamentally" so. If the hiring of an independent technical expert is intended to build public

[283] *See* Bridy, *ACTA and the Specter of Graduated Response*, *supra* note11, at 576-77 (highlighting the public law effects of the EMI-Eircom settlement and the ways in which such private settlements undermine consumer protection).

[284] LaFrance, *supra* note 138, at 167.

[285] *See* MOU, *supra* note 12, at 5 ("Failure to adopt a recommendation of the Independent Expert shall not amount to a breach under this Agreement.").

confidence in the quality of the technology underlying CAS, then the expert should be permitted to disclose any unremedied findings of inadequacy to the advisory board, which should be empowered to require the parties to act on the expert's findings. If the independent technical expert's findings can be disclosed only to the parties, which have no obligation to act on them, then there is very real reason to fear that those findings will simply be ignored. The independent expert's role in the system is not just to provide technical advice to the parties; it is to reassure the public of the parties' bona fides and the technology's integrity. Secrecy is not compatible with that dual role.

Secrecy is also the order of the day with respect to crucial aspects of the independent review program. As discussed in Part IV.C above, it appears that there will be no information forthcoming from CCI or AAA concerning the identity of the independent copyright expert or the "prevailing legal principles" of copyright law that will govern independent reviews. This information should be disclosed to the public on the CCI's web site. Lack of transparency with respect to the independent review program seriously compromises the public's perception of the fairness of the program and its independence from the copyright owner representatives, who are contractually entitled to bend the expert's ear on matters of substantive copyright law. Moreover, failing to publish the rules that will govern the independent review program is a missed opportunity to educate the public about copyright law, which is a stated purpose of CAS.

3. Outcomes

The MOU contains quite rigorous reporting requirements, but they are crafted to make the parties responsible to one another rather than the public. In keeping with that design, there is no role to play in outcomes assessment for the advisory board or any independent auditor. The reporting requirements associated with CAS exist primarily to enable CCI to verify the parties' compliance with their respective contractual obligations. Simply put, broadband subscribers are not among the MOU's intended information beneficiaries.

The MOU requires each participating ISP to generate monthly reports of anonymized and aggregated information concerning the number of alerts that were issued in the preceding month and the number of infringements alleged against each subscriber.[286] It also requires each ISP and each copyright owner group to make reasonable efforts to submit semi-annual reports to CCI about the results of CAS.[287] Using this information, CCI must conduct, on an annual basis, a program assessment that encompasses not only notice and sanction activity, but also the outcomes of independent reviews.[288] The MOU provides, in other words, for regular and thorough assessment of the entire CAS ecosystem on an ISP-by-ISP and copyright-owner-group-by-copyright-owner-group basis. All of this information flows into CCI, but it remains to be seen if any of it will flow out to the public in any form. Nothing in the MOU suggests that public disclosure about outcomes is an intended part of the program.

Secrecy is the norm under the MOU, and CCI's employees are sworn to silence when it comes to data disclosure. The MOU requires CCI to "maintain any reports or other information

[286] MOU, *supra* note 12, at 14-15.
[287] *Id.* at 18.
[288] *Id.* at 18-19.

provided hereunder in the strictest confidence" and prohibits CCI from "disclos[ing] such reports or information to any third party or any Party other than the Party which originated the report or information, absent written consent from the originating Party."[289] The MOU goes so far as to require CCI to seek a protective order from a court if information it has received from party becomes subject to a subpoena or other legal process.[290]

The level of secrecy maintained under the MOU with respect to program outcomes is excessive and, from a public relations standpoint, unproductive. At the very least, the advisory board should receive the semi-annual reports submitted to CCI by the parties and should be privy to the results of CCI's annual comprehensive assessment of CAS. Optimally, CCI would be required to compile and publish independently audited annual reports about program outcomes.

Conclusion

By the time this article goes to press, millions of Americans will already be subject to CAS, which is a model of graduated response that appropriately places more emphasis on education than on punishment. In what is ultimately a salutary development for consumers, CAS deviates from the "three strikes" orthodoxy that has dominated the global discourse on graduated response. With a longer educational arc and less severe sanctions than its French and Irish counterparts, CAS raises a hope that the global enforcement agenda could evolve to embrace more tempered mechanisms for managing online infringement. That would be a productive development in a domain where better enforcement is often wrongly equated with harsher punishment.

Measured against specific norms that are important to Internet users, however, CAS earns mixed marks. On the positive side, it does not involve content blocking or filtering, and it is unlikely to result in even a temporary suspension of Internet access for any accused repeat infringer. In addition, it does not require ISPs to monitor subscriber traffic or to turn over identifying information about individual subscribers to copyright owners. Finally, it provides an opportunity to appeal a finding of repeat infringement to an independent reviewer before any sanction is imposed, without foreclosing the possibility of judicial process.

On the negative side, there are insufficient safeguards in CAS to insure the accuracy of allegations of infringement, the fairness of the independent review process, and the independence and expertise of the various "independent experts" the MOU requires CCI to consult. Moreover, there is no way for the public to know whether the program is meeting the goals established for it in the MOU. Both Hadopi and Eircom have released information about outcomes, and it is incumbent upon CCI to follow suit. Increased informational transparency and an expanded role for the CCI advisory board in the ongoing operations of CAS would go a long way to alleviate many of these concerns.

[289] *Id.* at 19.
[290] *Id.*

The Graduated Response: Digital Guillotine or a Reasonable Plan for Combating Online Piracy?

by Danielle Serbin[1]

"With a [peer-to-peer file sharing] system, you can share your favorite songs with your best friend – or your 20,000 best friends."[2]

Online file sharing is great for users. It gives them free and easy access to millions of songs and movies with the click of a button. But file sharing is arguably harmful to the recording and film industries ("the industry"), precisely because it allows users to receive copyrighted works for free. In fact, the industry blames peer-to-peer file sharing for billions of dollars in lost revenue.[3] The industry has attempted to target online file-sharing with many different tactics, most prominently a mass-litigation campaign against end-users.[4] That campaign, largely considered a failure, ended in 2008.[5] In July 2011, the industry announced a new plan for targeting illegal file-sharing.[6] The plan is similar to a "three strikes and you're out" model used in many countries,[7] whereby users engaging in illegal file-sharing are given a warning for the first two instances of illegally sharing files, and on the third instance their Internet service is temporarily cut off.[8] The July graduated response deal is more of a "six strikes and you're maybe out" system.[9] The industry, in partnership with the major Internet Service Providers (ISPs), developed a program of six warnings of increasing intensity. For the first few instances of infringement, users will receive educational pamphlets, informing them that file-sharing is illegal and that there are legal routes to obtain movies and music online.[10] But for users who continue to file-share, the ISP will slow down or even cut off Internet access.[11] While some laud the program as an important step towards reducing online copyright infringement,[12] others refer to such a system as a "digital guillotine," because it "[kills] a critical way people connect with the world."[13]

This paper examines the July 2011 graduated response deal and concludes that it is not an optimal approach for addressing peer-to-peer file sharing–not for the industry, and not for the users. Part I briefly explains the technology of peer-to-peer file sharing technology and the reasons the industry wants to eliminate it (or more realistically, reduce it). Part II explains the industry's tactics for combating file sharing before the graduated response. It explains why the Digital Millennium Copyright Act (DMCA) – the provision of copyright law meant to address illegal Internet downloading – has not been a useful resource for preventing file sharing. Part III explains how because of DMCA's failure, the industry has had to use other means to target file sharing, most prominently a mass-litigation campaign against peer-to-peer file sharers, which proved to be both ineffective and hugely unpopular.

Part IV explains the July graduated response deal, and examines both the benefits and problems the program will create for users and the industry. It explains how it poses significant concerns for users because the graduated response allows ISPs to slow or cut off Internet access. Part IV argues that the problem with the graduated response is that the "punishment"

1. Third year law student, University of California Berkeley School of Law, Boalt Hall.

2. Lawrence Lessig, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* 54 (2004), http://www.jus.uio.no/sisu/free_culture.lawrence_lessig/portrait.letter.pdf.

3. *See* Part I, *infra*.

4. *See* Part III, *infra*.

5. Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, Wall Street J. (Dec. 19, 2008), http://online.wsj.com/article/SB122966038836021137.html?mod=rss_whats_news_technology.

6. Cornne McSherry & Eric Goldman, *The "Graduated Response" Deal: What if Users Had Been At the Table?*, Electronic Frontier Foundation (July 18, 2011), https://www.eff.org/deeplinks/2011/07/graduated-response-deal-what-if-users-had-been.

7. Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 Vand. J. Ent. & Tech. L. 695, 727 (2011) [hereinafter Bridy I] (*e.g.* the U.K., France, South Korea, and Taiwan).

8. *See* Peter K. Yu, *The Graduated Response*, 62 Fla. L. Rev. 1374 (2010).

9. *Memorandum of Understanding*, Center for Copyright Information 24 (July 6, 2011), http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf.

10. *Id.* at 8-9.

11. *Id.* at 10-13.

12. Nate Anderson, *White House: We "Win the Future" by Making ISPs into Copyright Cops*, Ars Technica (July 7, 2011), http://arstechnica.com/tech-policy/news/2011/07/white-house-we-win-the-future-by-making-isps-into-copyright-enforcers.ars.

13. William Patry, Moral Panics and the Copyright Wars 14 (2004).

doesn't match the "crime" – it slows or cuts off *all* of a user's Internet access *not* because the user fails to pay his or her bill, but because *some* of the user's activity allegedly infringes. And the graduated response system does all of this without providing the procedural safeguards an Internet user would otherwise receive in court. Further, Part IV explains the significant problems associated with slowed or terminated Internet access, chief among them impeding upon a user's freedom of expression and political assembly – two activities for which the Internet is a major forum.

Finally, Part V offers a potential alternative to the July graduated response deal. It advocates for a program that would have ISPs charge users a "file-sharing fee" for each instance of illegal file sharing, and then pass the proceeds onto the copyright holders. This approach is superior for the industry because it provides a quick and efficient mechanism for reducing losses incurred from peer-to-peer file sharing. And it is superior to the July graduated response deal for users because it does not cut slow or off Internet access.

I. Peer-to-Peer Sharing: What it is and Why the Industry Wants to Stop It

A. *Peer-to-Peer File Sharing Defined*

Peer-to-peer file sharing differs from music and movie downloading performed on a traditional client-server system. A client-server system is a "one way road," where users open a website and download a file directly from the website to their computers.[14] Peer-to-peer sharing is a two-way street; while you're online downloading other people's files, others using the sharing software can download files you have stored on your hardware.[15]

Peer-to-peer file sharing utilizes a software program to locate other computers that have files a user wants. File sharing occurs when: (1) the user logs in to a peer-to-peer file sharing software (such as Gnutella, BitTorrent, or The Pirate Bay); (2) the user requests files for download; (3) the software queries other computers that are connected to the Internet and also running the file-sharing software; (4) the program finds a computer with the requested file and downloads it directly to the user's hard drive.[16] This way, users are able to share songs and movies over the Internet with each other free of charge, without ever storing the material online or downloading it from a website.

B. *The Problem with Peer-to-Peer File Sharing*

Peer-to-peer file sharing violates copyright law because it infringes upon the copyright holder's exclusive rights of distribution and reproduction.[17] Many scholars argue that the current copyright framework is antiquated because it does not account for how easy modern technology makes reproduction and distribution (and hence infringement).[18] However, the law is clear that peer-to-peer file sharing is illegal, and Congress doesn't appear ready to change this. But simply because peer-to-peer file sharing is illegal does not mean it is necessarily harmful to copyright holders.

This paper works on the assumption that peer-to-peer file sharing is problematic and requires a solution. Not everyone agrees with this proposition. Some studies conclude that illegal file sharing does not negatively impact industry sales; some even argue that file sharing allows for greater "sampling" of recordings, which ultimately leads to greater sales.[19] However, there are many studies that conclude otherwise.[20] What is relevant for this Article is that both the movie and recording industries believe that peer-to-peer file sharing hurts sales and is worth combating. For example, in 2008, Michael Robinson of the MPAA

14. Carmen Carmack, *How BitTorrent Works*, HowStuffWorks (Mar. 25, 2006), http://computer.howstuffworks.com/bittorrent.htm; For a comprehensive the history of peer-to-peer file sharing, *see* Andrew W. Eichner, *File Sharing: A Tool for Innovation, or a Criminal Instrument?*, 2011 BCIPTF 1 (2011), *available at* http://bciptf.org/wp-content/uploads/2011/09/Andrew_Eichner_Note_File_Sharing_EICedits-final-edit.pdf.

15. *Id.*

16. *Id.*

17. *See* 17 U.S.C. § 106(1)-(3) (2006); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001). Notably, some scholars argue that when users simply make copyrighted works available by placing them in a shared folder on their computer, this does not necessarily constitute an illegal "distribution" under the Copyright statute, and courts misinterpret the law when they conclude that it does. *See, e.g.*, Andrew James McGarrow, *The "Making Available" Theory and the Future of P2P Networks: Does Merely Making Files Available for Further Distribution Constitute Copyright Infringement, and is it Time for Congress to Act in Accordance with this Technology?*, 88 U. Det. Mercy L. Rev. 155, 161 (2010).

18. *See, e.g.*, Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 Va. L. Rev., 813, 851 (2001).

19. John Schwartz, *A Heretical View of File Sharing*, N.Y. Times, Apr. 5, 2004, at C1.

20. *See, e.g.*, Alejandro Zentner, *Measuring the Impact of File Sharing on the Movie Industry: An Empirical Analysis Using a Panel of Countries*, 4 (Mar. 22, 2010), *available at* http://ssrn.com/abstract=1792615 (arguing that statistical evidence supports the conclusion that BitTorrent technology negatively impacts movie video sales).

(Motion Picture Association of America) stated that the movie industry loses "over $18 billion annually worldwide to piracy and Internet piracy . . . [i]t is a growing problem and a growing threat."[21] And according to the Recording Industry Association of America (RIAA), as of August 2008, "global theft of sound recordings cost the U.S. economy $12.5 billion in lost revenue and more than 71,000 jobs and $2 billion in wages to U.S. workers."[22]

II. Pre-Graduated Response Legal Framework: The DMCA Fails as an Efficient Mechanism for Combating Peer-to-Peer File Sharing

Most online downloading of copyrighted movies and music occurs not on traditional client-server websites, but through peer-to-peer file-sharing.[23] However, the DMCA, which is the legal mechanism for combating Internet copyright infringement, did not anticipate peer-to-peer file sharing. This is primarily because such file sharing did not exist in 1998 when Congress drafted the DMCA.[24] As such, Congress structured the DMCA to prevent Internet piracy through client-server illegal downloading.[25]

The DMCA provides safe harbor provisions to ISPs so long as they conform to certain statutory requirements.[26] These statutory requirements are meant to facilitate collaboration between ISPs and copyright holders so that infringing material can be removed from the Internet without a court order.[27] However, because Congress passed the DMCA before the advent of peer-to-peer file sharing, the DMCA is only effective at achieving this collaboration for illegal activity performed on client-server sites.[28]

The DMCA distinguishes between "storage providers," the traditional client-server sites (which served as host to most of the infringing activity when the DMCA was passed), and "conduit providers," which provide access to the peer-to-peer file sharers of today.[29] Storage providers are governed by DMCA § 512(c). They must comply with the DMCA's notice-and-takedown provisions.[30] This system works relatively simply: a copyright holder notices infringing material on a server, the copyright holder notifies the manager of server about the infringing material, and then the manager removes the material.[31] Further, under the "red flag" provision of the DMCA, even if a storage provider does not receive a notice of infringing material from a copyright holder, if it has knowledge of infringing material on its network, it must remove the material.[32] Thus, the DMCA is structured so that storage providers must work with the industry in order to maintain their safe harbor status.[33]

Unlike with storage providers, the DMCA provides "almost [an] absolute immunity from liability for transitory network communications . . . ."[34] The rationale for this is that, at least when the DMCA was created, conduit providers had no way of knowing whether infringing activity occurred over their systems. Conduit providers "route and transmit information without modifying it or storing it more than fleetingly."[35] Conduit providers fall under § 512(a) of the DMCA, and are not subject to the notice-and-take-down provisions of § 512(c).[36] Rather, to maintain their safe harbor status, conduit providers need only (1) adopt a policy that provides for the termination of access for repeat infringers in appropriate circumstances; (2) implement that policy in a reasonable manner; and (3) inform its subscribers of the policy.[37] Yet a conduit provider need not monitor

21. *Movie Industry Attacks Internet Downloading*, WCVBTV Boston (May 16, 2008), http://www.thebostonchannel.com/r/16274816/detail.html.

22. David Kravets, *MPAA Waffling on Piracy Costs; RIAA Says Illicit CDs Worth $13.74 Each*, Wired (Aug. 19, 2008), http://www.wired.com/threatlevel/2008/08/mpaa-waffling-o/ [hereinafter MPAA Waffling].

23. *See, e.g.*, McGarrow, *supra* note 17, at 180.

24. Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 Or. L. Rev. 81, 97 (2010) [hereinafter Bridy II]. Napster, the first popular file-sharing system, launched in July 1999. *See* Lessig, *supra* note 2.

25. Bridy II, *supra* note 24, at 97.

26. 17 U.S.C. § 512(a), (c) (2006).

27. Bridy I, *supra* note 7, at 713.

28. *Id.* at 719.

29. Bridy II, *supra* note 24, at 97.

30. § 512(c)(1)(A).

31. *See id.*

32. § 512(c)(1)(A)(ii). The law is still evolving regarding what constitutes a "red flag." *See, e.g.*, Viacom Int'l v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

33. Or else face suit for copyright infringement on multiple potential theories. For example, Viacom sued Google for direct copyright infringement, inducement to infringe, and contributory infringement. *See id.*

34. David Ludwig, *Shooting the Messenger: ISP Liability for Contributory Copyright Infringement*, B.C. Intell. Prop. & Tech. F.110701 (2006).

35. Bridy II, *supra* note 24, at 89.

36. *See* § 512(a); In re Charter Commc'ns, Inc., 292 F.3d 771, 776 (8th Cir. 2005) ("[T]he safe harbor provision [in § 512(a)], which limits the liability of an ISP when it merely acts as a conduit for infringing material without storing, caching, or providing links to copyrighted material[, does] not . . . contain the remove-or-disable-access provision. . . .").

37. Bridy II, *supra* note 24, at 90 (citing 17 U.S.C. § 512(i)(1)(A)); Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004).

its service or "affirmatively [seek] facts indicating infringing activity."[38] Therefore, even though a conduit provider must have an anti-infringement policy in place to maintain safe harbor status, the DMCA is not structured to promote collaboration between conduit ISPs and the industry in the same way it promotes collaboration between storage providers and copyright holders.

With the advent of peer-to-peer file sharing in the early 2000s, the industry faced a problem. Most infringing activity began occurring not on traditional client-server websites, but through peer-to-peer downloads.[39] But the industry had no means for addressing the problem in a quick, efficient manner, like it does when someone uploaded an infringing movie to YouTube.[40]

III. Before the Graduated Response: the Failed "War on Piracy"

In 2003, the RIAA began a campaign against online music theft – some referred to as a "war on piracy"[41] while others considered it a "anti-consumer crusade."[42] The MPAA began a similar campaign in 2005.[43] Notably, while the two organizations launched similar anti-piracy campaigns,[44] the RIAA's lawsuits against end-users were both more numerous and more widely publicized.[45] Both the RIAA and the MPAA used many tactics to combat peer-to-peer file sharing: developing an education campaign,[46] offering copyrighted works for download through legal means (through licenses with providers like iTunes),[47] and targeting websites that facilitated peer-to-peer file sharing such as Napster and Grokster.[48]

Part of the anti-piracy campaign involved suing end-users for peer-to-peer file sharing.[49] The RIAA sued an estimated 26,000 users through the campaign.[50] Almost all lawsuits resulted in the end-users settling with the industry, typically for $3,000 - $5,000,[51] or paying the statutory fine of (typically) $750 per song[52] as part of a default judgment.[53] However, in several high-profile lawsuits, the RIAA received huge jury verdicts against individual end-users. These included a $675,000 verdict against a 25-year-old graduate student for illegally downloading 30 songs[54] and a $1.5 million verdict against a Minnesota woman for illegally downloading 24 songs.[55]

The war was widely unpopular due to harsh penalties, what some called "strong arm" enforcement policies, and misidentified or ill-targeted end-users.[56] Among the targets of RIAA's suits were "several single mothers, a dead person[,] a 13-year-old girl[,]"[57] and a

38. 17 U.S.C. § 512(m)(1).

39. *See, e.g.*, McGarrow, *supra* note 17, at 180.

40. *See* 17 U.S.C. § 512(c) (2006).

41. McBride & Smith, *supra* note 5.

42. *How To Not Get Sued for File Sharing*, Elec. Frontier Found. (Jul. 1, 2006), https://www.eff.org/wp/how-not-get-sued-file-sharing.

43. Bary Alyssa Johnson, *MPAA Anti-Piracy Lawsuits Target Individuals*, PC Magazine (Aug. 29, 2005, 04:32 PM), http://www.pcmag.com/article2/0,2817,1853573,00.asp#fbid=kCTuxJnUIgJ.

44. For example, they were both plaintiffs in MGM v. Grokster, 543 U.S. 913 (2005).

45. *See, e.g.*, Brett Caraway, *MPAA Talks to Copygrounds About P2P File Sharing and Copyright*, Copygrounds (Oct. 25, 2010), http://copygrounds.com/2010/10/05/mpaa-talks-to-copygrounds-about-p2p-file-sharing-and-copyright/ (stating that Fritz Attaway, Executive Vice President and Special Policy Advisor for the MPAA, said the MPAA does target end-users, but due to the nature of the respective copyrighted material, the MPAA has filed fewer suits against end-users than the RIAA).

46. Daniel Reynolds, *The RIAA Litigation War on File Sharing and Alternatives More Compatible with Public Morality*, 9 Minn. J.L. Sci. & Tech., 977, 978 (2008); *see also* Caraway, *supra* note 45.

47. *See* Caraway, *supra* note 45; Kelly Leong, *iTunes: Have They Created a System for International Copyright Enforcement?*, 13 New Eng. J. Int'l & Comp. L. 365, 384 (2007) (stating that Apple obtained "licensing agreements from five major record labels—EMI, Sony, BMG, Vivendi-Universal and AOL/Time-Warner—and licensing agreements with independent record labels").

48. *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); M.G.M. v. Grokster, 545 U.S. 913 (2005).

49. *See* Reynolds, *supra* note 46, at 981.

50. *Id.*

51. *See* Jonathan Salzman, *Trial to Begin in Music Copyright Case*, Boston.com (Jul. 28, 2009), http://www.boston.com/news/local/massachusetts/articles/2009/07/28/four_record_labels_suing_bu_student/; Yu, *supra* note 8, at 1390 (explaining what defendants face with, what Lawrence Lessig refers to, a "'mafia-like choice" between a costly settlement and an outrageously high legal bill incurred in defending the lawsuit").

52. *See* 17 U.S.C. § 504(c)(1)-(2) (2006) (statutorily, damages can range from $200 - $150,000 per infringement, depending on the willfulness of the infringement and at the court's discretion).

53. *See* Reynolds, *supra* note 46, at 980-984 (explaining in detail the life-cycle of a RIAA suit against an end-user); *see also* Ray Beckerman, *How the RIAA Litigation Process Works*, Ray Beckerman PC (Apr. 9, 2008), http://beckermanlegal.com/howriaa.htm.

54. Denise Lavoie, *Joel Tenebaum: Jury Awards $675,000 in Boston Music Downloading Case*, Huffington Post (Jul. 31, 2009, 08:37 PM), http://www.huffingtonpost.com/2009/07/31/joel-tenenbaum-jury-award_n_249155.html.

55. *See* David Kravets, *Judge Slashes 'Appalling' $1.5 Million File Sharing Verdict to $54,000*, Wired (July 22, 2011, 2:29 PM), http://m.wired.com/threatlevel/2011/07/kazaa-verdict-slashed.

56. *See* Matthew Sag, *Piracy: Twelve Year-Olds, Grandmothers, And Other Good Targets For The Recording Industry's File Sharing Litigation*, 4 Nw. J. Tech. & Intell. Prop. 133, 133 (2006); *see also* McBride & Smith, *supra* note 5 (referring to the suits against end-users as a "public relations nightmare").

57. *See* Sag, *supra* note 57, at 146; Anders Bylund, *RIAA Sues*

family without a computer.[58] One target of an MPAA suit was a 67-year old Wisconsin grandfather whose grandson illegally downloaded four movies.[59]

To properly assess the results of the industry's mass-litigation campaign, two questions must be examined. First, did the campaign decrease illegal file-sharing of copyrighted material? And second, did the campaign correspond to a decrease in losses suffered by the industry? There is inconsistent evidence regarding the first question.[60] But, while studies yield differing results when it comes to whether internet downloading decreased after the industry's mass-lawsuit campaign, there is widespread agreement that the industry's anti-piracy campaign did very little, if anything, to stop the downward trend in sales.[61] The "RIAA [sic] reported declining revenue in nine [out of ten years between 2000-2010], with album sales falling an average of 8% each year."[62] No doubt, other factors contributed to this decline,[63] but the RIAA clearly attributes much of it to online piracy. In 2008, the year the RIAA ended its mass-litigation campaign,[64] the RIAA stated that "global theft of sound recordings cost the U.S. economy $12.5 billion in lost revenue and more than 71,000 jobs and $2 billion in wages to U.S. workers."[65] The film industry did not experience a similar overall decline in sales (not consistently over the years and among its various markets (i.e., home video, box office)),[66] but in 2008 an MPAA report stated that Internet piracy cost the film industry $7 billion.[67] Further, in 2010 the MPAA stated that online piracy costs the creative industries "billions of dollars" and threatens the job security of "hundreds of thousands" of Americans.[68]

Therefore, the industry's mass-litigation campaign was not effective in deterring peer-to-peer file sharing. Years after the campaign began, both music and movie industry representatives continued to claim that piracy is wide-spread and costs them billions of dollars in lost revenue.

In fact, there is evidence that the mass-litigation campaign *added* to the net losses suffered by the industry:

> [T]he lawsuits did not increase the payments to artists by even one penny. Overall, in terms of revenues these lawsuits had little, if any, effect. The majority of [the lawsuits] were settled for amounts ranging from $3,000 to $11,000, while the cost of pursuing these lawsuits has often exceeded these sums.[69]

Another study concluded that RIAA recovered only 2% of the money it spent on lawsuits through settlements and verdicts against end-users.[70]

IV. The July 2011 Graduated Response Deal

A. *Why the Deal?*

When it publicly announced an end to its mass-litigation campaign, the RIAA also announced its interest in working with ISPs to implement a graduated response system.[71] But the ISPs initially denied interest in the program.[72] In fact, as recently as March 2010,

---

Computer-Less Family, 234 Others, for File Sharing, ARS TECHNICA (Apr. 24, 2006), http://arstechnica.com/old/content/2006/04/6662.ars.

58. *Id.*

59. Nate Mook, *MPAA Offers Deal to Sued Grandfather*, BETANEWS (Nov. 4, 2005), http://betanews.com/2005/11/04/mpaa-offers-deal-to-sued-grandfather/.

60. *See* Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 CARDOZO ARTS & ENT. L.J. 725, 736-745 (2005) (summarizing empirical studies reaching both a positive and negative result); *see also RIAA v. The People: Five Years Later*, ELECT. FRONTIER FOUND., 9 (2008), http://www.eff.org/files/eff-riaa-whitepaper.pdf.

61. Interestingly, if the studies arguing that illegal Internet downloading decreased due to the mass-litigation campaign are correct, this might mean that (as some argue) illegal downloads of copyrighted materials have little effect on music and movie sales.

62. *See* David Goldman, *Music Industry's Lost Decade: Sales Cut in Half*, CNN.COM (Feb. 3, 2010), http://money.cnn.com/2010/02/02/news/companies/napster_music_industry/.

63. *See id.* (stating that "the two recessions during the decade certainly didn't help music sales. It's also a bit unfair to compare the 2000s with the 1990s, since the '90s enjoyed an unnatural sales boost when consumers replaced their cassette tapes and vinyl records *en masse* with CDs").

64. *See* McBride & Smith, *supra* note 5.

65. *See* MPAA Waffling, *supra* note 22.

66. *See, e.g.*, Jacqui Cheng, *DVD sales tank in 2009 as Americans Head to the Cinema*, ARS TECHNICA (Jan. 4, 2010), http://arstechnica.com/media/news/2010/01/dvd-sales-tank-in-2009-as-americans-head-to-the-cinema.ars.

67. *See* MPAA Waffling, *supra* note 22.

68. *See* Motion Picture Ass'n of Am. Reply Comments at 5-6, In re Preserving the Open Internet Broadband Indus. Practices, 24 F.C.C.R. 13064 (2009), *available at* http://www.mpaa.org/Resources/46ba617a-4dc9-4fdb-acce-9100ac274af4.pdf.

69. Lital Helman, *When Your Recording Agency Turns into an Agency Problem: The True Nature of the Peer-to-Peer Debate*, 50 IDEA 49, 65 (2009).

70. *See* Mike Masnick, *RIAA Spent $17.6 Million In Lawsuits... To Get $391,000 In Settlements?*, TECHDIRT (Jul. 14, 2010, 09:44 AM), http://www.techdirt.com/articles/20100713/17400810200.shtml.

71. *See* McBride & Smith, *supra* note 5.

72. *See* David Kravets, *Top Internet Providers Cool to RIAA*

a Verizon representative publicly disavowed ISP involvement in a graduate response: "the government and the courts, not ISPs, are responsible for intellectual property enforcement, and only they can secure and balance the various property, privacy, and due process rights that are at play and often in conflict in this realm[.]"[73] However, other ISPs appeared more interested in a graduated response system. For example, in 2009, AT&T publicly admitted to taking part in a "trial" graduated response system.[74] And in July 2011, all of the major ISPs (including Verizon) formally agreed to the graduated response deal with the MPAA and the RIAA.[75] No consumer groups took part in negotiating the graduated response.[76]

It is not clear why the ISPs changed their tune and agreed to collaborate with the industry on the graduated response. None of the ISPs have provided much of a public explanation about the shift in policy. Below is a of list various theories to explain this shift in policy – the reality is likely a combination of them all.

1. The Government Made Them Do It

Notably, though the ISPs are passive carriers under the DMCA and have significant safe harbor protection, nothing prevents Congress from amending the DMCA to alter this protection. So it is in the ISP's best interest to cooperate with government pressure. Recently released e-mails between the U.S. Intellectual Property Enforcement Coordinator, Victoria Espinel, and the industry and ISP leaders reveal that the government was very involved and brought the parties to the table, encouraged the deal, and was kept in the loop regarding the terms of the deal.[77]

2. ISPs have a Closer Relationship with the Industry than in the Past

"Eight years ago, the Recording Industry Association of America had to sue Verizon to try to uncover the identity of a customer who was sharing music online," but now the industry enjoys a much more collaborative relationship with ISPs.[78] For example, Comcast owns a majority stake in NBC Universal, and studios license movies to cable providers as part of video on-demand service. "The [ISPs] want to cooperate with Hollywood because the carriers recognize that their own growth depends in part on bundled content strategies . . . [t]hey don't want to be just utilities providing Internet access, but premium content distributors as well."[79]

3. No Longer "Dumb Pipes"

As mentioned in Part II, ISPs have traditionally been considered passive carriers and therefore enjoy the strongest safe-harbor protections in the DMCA. But this may be changing because of (a) the ISPs recent implementation of website-filtering technology and (b) a recent district court decision holding that a passive carrier who engages in filtering is not eligible for § 512(a) safe harbor status.

Many ISPs now implement "Deep Packet Inspection" (DPI) technology, which allows them to examine a user's Internet activity in great detail and to block access to certain websites.[80] ISPs are interested in DPI technology for many potential reasons unrelated to copyright infringement: "DPI can be used . . . for detection and filtering of viruses and malware, management of network congestion," "traffic sorting," "data mining," and for "law enforcement purposes, as required by the Communications Assistance to Law Enforcement Act (CALEA), to capture and transmit data to government agents."[81]

In *Arista Records LLC v. Usenet.com, Inc.*[82] the court held that Usenet.com, a website that acted

3-Strikes Plan, WIRED (Jan. 5, 2009, 11:43 AM), http://www.wired.com/threatlevel/2009/01/draft-verizon-o/.

73. *See* Bridy I, *supra* note 7, at 730 (citing Letter from James W. Cicconi, AT&T executive, to Victoria Espinel (March 24, 2010)).

74. *See* Sarah McBride, *Relationship Status of RIAA and ISPs: It's Complicated*, WALL ST. J. DIGITS BLOG (Mar. 26, 2009), http://blogs.wsj.com/digits/2009/03/26/relationship-status-of-riaa-and-isps-its-complicated/.

75. Antony Bruno, *Labels Reach Deal With ISPs on Antipiracy Effort*, BILLBOARD (July 7, 2011), http://www.billboard.biz/bbbiz/industry/legal-and-management/labels-reach-deal-with-isps-on-antipiracy-1005267702.story.

76. *See* McSherry, *supra* note 6.

77. *See* David Kravets, *U.S. Copyright Czar Cozied Up to Content Industry, E-Mails Show*, WIRED (Oct. 14, 2011, 06:30 AM), http://www.wired.com/threatlevel/2011/10/copyright-czar-cozies-up/#more-31071; *see also* Anderson, *supra* note 12 (stating "while ISPs were for years seen more like the 'common carriers' of yore, who ran a network and were generally not responsible for policing the uses of that network, government sentiment in key quarters is changing").

78. Ben Sisario, *To Slow Piracy, Internet Providers Ready Penalties*, N.Y. TIMES, Jul. 7, 2011, http://www.nytimes.com/2011/07/08/technology/to-slow-piracy-internet-providers-ready-penalties.html?pagewanted=all.

79. *See* Nate Anderson, *Judge Throws Book at Usenet.com in RIAA Lawsuit*, ARS TECHNICA (July 1, 2009, 12:00 PM), http://newsystocks.com/News/4099511/Pirates-of-the-Web-in-Trouble.

80. *See, e.g.*, Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J., 633, 656 (2008); *see also* Bridy II, *supra* note 24, at 104.

81. Bridy II, *supra* note 24, at 104.

82. 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

are they monitoring (DPI) or just passing along notices + shutting the card

as a "'common carrier' delivering requested files to subscribers without active involvement"[83], was not eligible for the DMCA § 512(a) safe harbor provision.[84] Though superficially Usenet.com appeared to be a passive carrier (i.e., it did not store user's uploaded files), the court noted that Usenet "took active measures to create servers dedicated to MP3 files and to increase the retention times of newsgroups containing digital music files."[85] Further, "Usenet.com also took [many] steps to control subscriber access to material, including automated filtering and human review to block pornography and block access to certain users."[86] Because of the *Usenet* decision, some commentators and scholars concluded that "[w]hile monitoring by itself may not eliminate the safe harbor qualification, deep packet monitoring probably does because the packet header information likely will identify significant information about the nature and type of traffic sufficient to put the ISP on actual notice of any copyright infringement."[87] So ISPs may have been more willing to implement the graduated response because, due to DPI, they no longer are immune credible claims of direct copyright infringement. Their rationale may have been that it is better to collaborate with the industry than be sued by it.

Was Used a Company

4. Jumping on the "International Bandwagon"

Oh did not realize other

The "U.K., France, South Korea, and Taiwan have already incorporated a graduated response into their domestic copyright enforcement systems," and "[s]imilar legislation is making its way through the legislative process in New Zealand . . . ."[88] And in May 2010, one of Ireland's major ISP providers, Eircom, instituted a graduated response policy.[89] The fact that ISPs abroad were willing to collaborate with the industry in combating Internet piracy may have signaled to U.S. ISPs that the graduated response is a worthwhile endeavor.

B. The Graduated Response Memorandum of Understanding ("MOU")

On July 6, 2011, the major ISPs[90] signed a "Memorandum of Understanding" (MOU) with the RIAA and the MPAA,[91] implementing a graduated response system in the U.S.. The graduated response system as set forth in the MOU is a sort of "six strikes and you're maybe out" system. The most notable features of the system are as follows:

- Establishment of the Center for Copyright Information (CCI) to oversee implementation of the graduated response.[92] The CCI is governed by a six member executive committee, with three members designated by copyright owners and three members designated by the participating ISP's.[93] The CCI also has a three member advisory board, with one representative chosen by the copyright holders, one by the ISPs, and the last chosen by those two members. The advisory board members are not employees of the ISPs or industry players, but rather will be experts from the subject matter area and consumer interest communities.
- A six-step "Copyright Alert" system, involving three stages:[94]

83. Bridy II, *supra* note 24, at 122.

84. *Usenet.com*, 633 F. Supp. 2d at 148-49.

85. *Id.* at 148.

86. Anderson, *supra* note 79.

87. Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, PENN. STATE UNIV., http://www.personal.psu.edu/rmf5/Net Neutrality and IPR.htm.

88. Bridy I, *supra* note 7, at 727. While most international graduated response systems are government-run (unlike the July U.S. deal), they still require ISP involvement.

89. *ISP Introduces "Graduated Response" Leading to Disconnection for Illegal Downloaders*, REPORTERS WITHOUT BORDERS (May 28, 2010), http://en.rsf.org/ireland-isp-introduces-graduated-response-28-05-2010,37583.html.

90. *Memorandum of Understanding*, *supra* note 9, at 21-23. The participating ISPs include: SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Inc., Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies); Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies); Comcast Cable Communications Management, LLC; CSC Holdings, LLC (solely with respect to its cable systems operating in New York, New Jersey, and Connecticut) (the Cablevision systems); and Time Warner Cable Inc.

91. *Id.* at 25. The members of said Associations listed as participating are: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc.; Recordings, Inc., Warner Music Group, Sony Music Entertainment, and EMI Music North America.

92. *Id.* at 3-6.

93. *Id.* at 3.

94. *Id.* at 7-13. The ISPs have some discretion about when to implement each measure. An ISP responds to the first instance of alleged infringement with the Educational Alert. It can respond

- First stage – Information Alert(s): at this stage, the ISP notifies the subscriber of his/her infringement. The ISP sends a notice to the alleged infringer with the following information: (a) copyright infringement is illegal; (b) users must not engage in illegal infringement; (c) there are lawful methods of obtaining copyrighted works; (d) continuing and subsequent receipt of alerts may result in the ISPs taking action by the application of mitigation measures; (e) in addition to these Mitigation Measures, the Participating ISP may also temporarily suspend or terminate Internet service; and (f) information regarding how to challenge the "Copyright Alerts" – CCI's appeal process. The ISP issues the Information Alert after the first and second instances of alleged copyright infringement.[95]

- Second Stage - Acknowledgment Alert (for a user's third and fourth alleged infringements): This alert is similar to the educational step, but it requires the user to acknowledge receipt of the alert (through a click-through mechanism, a landing page, or a pop-up page).[96]

- Third Stage - Mitigation Measures (for a user's fifth and sixth alleged infringements): At the ISP's discretion, it can take one of the following steps: temporary reduction in uploading and/or downloading transmission speeds; temporary redirection to a landing page until the user contacts his/her ISP to discuss the Copyright Alerts; or temporary restriction of the user's Internet access.[97]

- Importantly, at none of the stages *must* the ISP cut off Internet access, though it can. Similarly, should the ISP cut off Internet access, at its discretion it need not disable a user's IP voice service (VOIP), e-mail account, security service, health service (i.e., home medical monitoring), or Internet video programming service.[98]

- A system of what the MOU labels "independent review" for users with who challenge the notification on any one of six grounds: (1) misidentification of account; (2) unauthorized use of account; (3) the use of the copyright work was authorized by the copyright owner; (4) fair use; (5) misidentification of file; or (6) copyrighted work was published before 1923 (and is in the public domain).[99]

- Users must pay a filing fee of $35 to invoke review, and must electronically submit their complaint within ten business days of receiving the Copyright Alert.[100]

- The "independent reviewer" will be an attorney chosen by a "panel of neutrals," and the review process "will, to the extent relevant, apply prevailing legal principles as determined by the United States federal courts."[101]

1. Problems with the MOU

The parties to the MOU claim that it "seeks to establish a consumer-focused process for identifying and notifying" users of infringing activity, and that the primary goal of the MOU is to "educate consumers, deter online infringement, and direct consumers to lawful online legitimate sources of content."[102] However, though it may be consumer-*focused*, the MOU contains numerous provisions that are not consumer-*friendly*.

to the second instance of alleged infringement with either the Educational Alert or the Acknowledgment Alert, at its discretion. The ISP responds to the third and fourth instances of copyright infringement with the Acknowledgment Alert. Upon receiving notice of a fifth instance of alleged infringement, the ISP can either issue another Acknowledgment Alert or can implement the Mitigation Measures. The Mitigation Measures are not waivable for the sixth instance of alleged infringement, however. Further, the system is reset after a year: whatever measures have been taken against a user, after a year of non-infringing activity the number of infringements is reset back to zero.

95. *Id.* at 8-9
96. *Memorandum of Understanding*, *supra* note 9, at 9-10.
97. *Id.* at 10-13.
98. *Id.* at 12.
99. *Id.* at 26.
100. *Id.* at 30.
101. *Id.* at 31, 33, 35.
102. *Memorandum of Understanding*, *supra* note 9, at 2.

The MOU is certainly an improvement over the industry's former tactic of targeting unassuming, and sometimes ignorant, end-users with lawsuits after what was often only minimal file sharing. The MOU's focus on education over punishment – at least with the first measure – helps to inform unassuming consumers who may simply not know that peer-to-peer file sharing is considered copyright infringement by the industry.[103] In fact, according to the RIAA, over 25% of Americans still do not know peer-to-peer file sharing is illegal.[104] But the central problem created by the MOU is that it allows an ISP to slow or cut off users' Internet without ensuring them either due process or neutral enforcement.

Notably, the MOU does not require ISPs to cut off Internet service. But it does not stop them from doing so. And its other "mitigation measures" short of cutting off service – for example, slowing service – are similarly harmful to Internet users. This is because cutting off Internet access is not like stopping a cable TV service if a user does not pay his monthly bill. It denies its users access to a fundamental part of their daily lives – the Internet – and basic civil rights associated with the Internet like speech and assembly – not because users fail to pay their Internet bill, but because of allegedly illegal Internet activity.

While Internet access is not recognized as a civil right in the US,[105] the Internet has been compared to a civil right even by the ISPs: David Cohen, Comcast's executive vice president, stated that "[a]ccess to the [I]nternet is akin to a civil rights issue for the 21st century[; it is] that access that enables people in poorer areas to equalize access to a quality education, quality health care and vocational opportunities."[106] Further, there is a clear trend towards expanding Internet access; for example, "in 2009 [Congress] appropriated $4.7 billion in economic stimulus funds to enhance the [U.S.] broadband infrastructure and expand access to underserved populations."[107] Thus, because Internet access is an essential component of daily modern life, "termination of Internet access represents a powerful and far-reaching sanction that directly impacts" the "ability of Internet users to consume media, their ability to work, learn, communicate, manage finances, and participate in the collective life of society."[108]

Additionally, the Internet is inextricably linked to numerous already-existing civil rights, chief among them the First Amendment rights of expression and assembly. For example, a Pew Research study concluded that 56% of those involved in a civic or political group used the Internet to communicate with other group members.[109] Current jurisprudence does not consider ISPs state actors.[110] Thus, while in *Reno v. ACLU*, the Supreme Court held that while the government cannot substantially restrict speech via the Internet, no law prevents ISPs from doing so.[111] So a user whose Internet is cut off cannot sue ISPs for violating the user's rights to speech and assembly, even though the Internet is many people's primary forum for both.

Further, the MOU provides users very little in the way of procedural protections. The MOU raises three primary process-related concerns. First, it deprives users of due process they would otherwise get in a federal court. The MOU flips many traditional principles of due process on their head. In the graduated response system, the industry is in essence the "plaintiff" and the users are the alleged "defendant infringers." The burden of proof, however, is on the user, as is the filing fee.[112] Further, the user only has ten days to perform research to mount its defense – hardly enough time when going up against industry-backed lawyers in an industry-created system. A second problem with the MOU is that it restricts the universe of potential defenses to copyright infringement to six defined defenses, which do not cover the entire universe

103. However, the neutrality of the educational measures is unclear. It is likely that the education will be one-sided as it is coming from the industry; still, for consumer advocates, this is preferable to a system that penalizes users with costly settlements, default judgments, or jury verdicts.

104. *For Students Doing Reports*, RIAA, *http://www.riaa.com/faq.php* (last visited Feb. 19 2012).

105. Finland recently became the first nation to make Internet access a legal right. *First Nation Makes Broadband Access a Legal Right*, CNN.COM (July 1, 2010), http://articles.cnn.com/2010-07-01/tech/finland.broadband_1_broadband-access-internet-access-universal-service?_s=PM:TECH.

106. Christopher Mitchell, *Comcast: Internet Access Is Temporarily a Civil Right*, HUFFINGTON POST (Aug. 9, 2011), http://www.huffingtonpost.com/christopher-mitchell/comcast-internet-access-i_b_921608.html.

107. Bridy II, *supra* note 24, at 125-26.

108. *Id.* at 126.

109. Aaron Smith, *Civic Engagement Online: Politics as Usual*, PEW RESEARCH CTR. (Sept. 1, 2009), http://pewresearch.org/pubs/1328/online-political-civic-engagement-activity.

110. *See, e.g.*, Noah v. AOL Time Warner Inc., 261 F.Supp.2d 532 (E.D. Va. 2004); Langdon v. Google Inc., 474 F. Supp. 2d 622 (D. Del. 2007).

111. 521 U.S. 844 (1997).

112. See Bridy I, *supra* note 7, at 729 (noting "there is a significant risk of abuse inherent in a system that streamlines enforcement by dispensing with the neutral adjudication of claims").

of potential copyright defenses.[113]

A third problem presented in the MOU is enforcement. Though the procedural mechanisms the MOU has in place are lacking, perhaps an even bigger problem for users is that there is no guarantee that the CCI will follow those procedures. As mentioned, the government was very involved in brokering the MOU, and if the CCI threw its procedural handbook out the window, it is likely the government would pressure the industry and ISPs to get back in line. However, because the MOU is essentially a contract between two private entities – the ISPs and the industry – compliance simply cannot be guaranteed.

V. An Alternative to the July Graduated Response MOU

Because the MOU threatens user's Internet access, threatens the rights associated with Internet access, and provides users no promise of due process in doing so, this Article recommends that a different system be adopted. This Article recommends modifying the graduated response to a system of two warnings followed by charging the user a fee for every subsequent file-sharing instance.

A system that imposes fines for each instance of illegal downloading is superior to the plan outlined in the MOU. Like in the MOU, this system would begin with the copyright holder notifying the ISP of infringing activity. Then, for the first two instances of infringement, the ISP will issue the user a warning. This warning will consist of a notification, an educational pamphlet, and information that the user will be charged if he continues to file-share (much like "Information Alerts" outlined in the MOU). After the first two instances of infringement, the ISP will charge the user a fee for each instance of illegal downloading. The charges will show up on the user's monthly bill. The ISPs and industry groups (preferably in collaboration with consumer groups) can determine reasonable fees; they might even agree on graduating the fees with each infringing activity. The ISPs will then pass on most of the proceeds from the fees (as agreed upon with the industry) to industry groups.

This sharing-fee system is preferable to the plan in the MOU for all parties. First, a fee-sharing system does not slow or cut down Internet access. It is a system where, to the extent there is a punishment for file sharing, the punishment fits the crime. Rather than taking away all Internet access for continued infringing activity, a user would merely be charged in relation to his activity.

Second, the sharing-fee system provides the industry immediate financial compensation for Internet file-sharing. As mentioned, the MOU does no more than deter file sharing with hopes that users will change their ways and download music legally. A fee has the same deterrent effect, and provides the industry *direct* compensation for losses associated with Internet piracy. In fact, so long as the fine is more than the typical cost of a song or movie download (about $1 and $15, respectively)[114], the industry could conceivably *profit* from illegal downloads (or more realistically, break even).

The sharing-fee system is also preferable for ISPs, who will not have to impose the harsh mitigating measures outlined in the MOU. While consumers may balk at the fines and blame the messenger, so long as the fees are reasonable and are explained on the bill and in an accompanying educational pamphlet, it is unlikely that the backlash will result in lost customers, at least not any more lost customers than would be the result of a policy that slows or cuts off Internet speed.

A sharing-fee system is not without flaws. For instance, it might be conceived as quasi-punitive because of the fees it levies on users. But despite this flaw, an important aspect of the sharing-fee system is that it does not deprive users of a fundamental element of their daily lives – the Internet. Further, some of the same process and misidentification issues that plagued the industry's mass litigation campaign might still exist with this sharing-fee system. To address this, the ISPs should adopt an appeals system that grants the user all of the defenses to copyright infringement the user would have in a court of law. Moreover, due process concerns are less prevalent in a system that does not deprive users Internet access. Another potential problem with the sharing-fee system is that it may hit poorer users harder than wealthy ones. No doubt, if a user cannot pay his or her Internet bill due to hundreds of dollars in sharing-fees, the ISPs will cut off their service. So the end result of the sharing-fees system *could* be the same as the mitigation measures outlined in the MOU. However, slowing Internet

113. McSherry, *supra* note 5.

114. Dawn C. Chmielewski, *iTunes embraces 3-tier pricing, will remove anti-copy software*, L.A. Times, Jan. 7, 2009, http://articles.latimes.com/2009/jan/07/business/fi-itunes7 (showing that on iTunes, songs cost either 69 cents, 99 cents, or $1.29); *Frequently Asked Questions (FAQ) for purchased movies*, Apple, http://support.apple.com/kb/HT1906 (last visited Mar. 26, 2012) (showing that on iTunes, movie prices range from $9.99 to $14.99).

service is not part of the sharing-fee system, and cutting off service will not be at the ISPs' discretion, but only if users do not pay their Internet bill. Moreover, any appeal process under this sharing-fee system should be structured to allow a user to appeal before the bill is due rather than after. This process could be akin to the process of appealing a contested credit card charge, which results in no penalty.

A sharing-fee system is both most efficient for the industry and most protective of user's interests. While the industry chose not to implement a similar proposal posited in the mid-2000s–a voluntary licensing scheme that would allow file-sharing in return for a monthly fee[115]–it may be more receptive to a sharing-fee system now. Unlike a licensing system, a sharing-fee system would not require the industry to work directly with millions of end-users, which addresses issues of efficiency.[116] And the requisite collaboration with the ISPs is already in place thanks to the MOU, making the sharing-fee system easy to implement.

Importantly, a sharing-fee system where infringers pay copyright holders for infringing activity is much more in-line with traditional conceptions of U.S. copyright law than is the current plan outlined in the MOU. In the United States, copyright has traditionally been conceptualized as an economic right, not a moral right. The theory behind moral rights "is that authors of copyrightable works have inalienable rights in their works that protect their moral or personal interests."[117] If copyright law is conceived of as a moral right, then it makes more sense to have a system like the MOU in place – a system that punishes those who infringe on another's personhood rights by taking away some of the infringer's personhood rights, in the present case those rights are Internet access and the expression and assembly rights associated with it. But in the United States, copyright infringement is conceptualized as infringing upon a copyright holder's exclusive monopoly to exploit the creator's work for economic gain. If copyright law is conceptualized in this way, it makes more sense to charge the infringer a sum of money for infringement and place these funds back in the copyright holder's hands.

VI. Conclusion

Though a worthy attempt to target Internet piracy of films and music, the 2011 Graduated Response system ultimately levies severe penalties upon end-users for illegal downloads. These penalties include slowing and potential cut-off of Internet access. Moreover, the MOU does not ensure sufficient procedural protections for users. Instead, a sharing-fee system that charges users in proportion to their infringing downloads would place less of a burden on users and result in greater efficiency and financial recovery for the music and movie industries.

115. Jason Schultz, *File Sharing Must be Made Legal*, Salon (Sept. 12, 2003), http://www.salon.com/2003/09/12/file_sharing_two/.

116. On the challenges of administering a voluntary licensing system to end-users, *see* Meghan Dougherty, *Voluntary Collective Licensing: The Solution to the Music Industry's Crisis?*, 13 J. Intell. Prop. L., 405, 429 (2006).

117. Cyrill P. Rigamonti, *Deconstructing Moral Rights*, 47 Harv. Int'l L.J., 353, 355 (2006).

The Effect of Graduated Response Anti-Piracy Laws on Music Sales:
Evidence from an Event Study in France

Brett Danaher[‡]
Wellesley College, Department of Economics

Michael D. Smith[†]
Carnegie Mellon University, Heinz College

Rahul Telang[†]
Carnegie Mellon University, Heinz College

Siwen Chen[‡]
Wellesley College, Department of Economics

This Version: March 2012

Acknowledgements: The authors thank four major record labels for generously providing data to support this research. Smith and Telang acknowledge generous support from Carnegie Mellon's iLab. While this research was undertaken independently, the IFPI has compensated Danaher for his time to present the results of this study to the IFPI and to produce a non-technical version of this paper for their internal use. We also thank Adeline Tan and Ljubica Ristovska for excellent research assistance.

---

‡ Department of Economics, Wellesley College, Wellesley, MA, 02481
† School of Information Systems and Management, Heinz College, Carnegie Mellon University, Pittsburgh, PA, 15213.

The Effect of Graduated Response Anti-Piracy Laws on Music Sales:
Evidence from an Event Study in France

ABSTRACT

Digital piracy is seen as a significant problem for the creative industries. Still, while there have been many academic studies showing that piracy hurts sales, there have been far fewer studies analyzing the effectiveness of anti-piracy measures in reversing this effect. This study attempts to address this question by analyzing how the HADOPI "three strikes" law in France affected digital music sales on the iTunes music store.

To do this, we obtained a panel of iTunes sales data from the four major music labels (Universal Music, Warner Music, EMI Music and Sony Music) across a broad set of countries. We then applied a difference-in-difference approach, using sales trends in a control group of European countries to simulate the counterfactual of what music sales in France would have been if HADOPI had not been passed. Our results suggest that increased consumer awareness of HADOPI caused iTunes song and album sales to increase by 22.5% and 25% respectively relative to changes in the control group.

In terms of robustness, we find that these sales changes are similar for each of the four major music labels, suggesting that our results are not peculiar to any particular label. We also find that the observed sales increase is much larger in genres that, prior to HADOPI, experienced high piracy levels (e.g., Rap and Hip Hop) than for less pirated genres (e.g., Christian music, classical, and jazz). This strengthens the causal interpretation of our results since if HADOPI is causing pirates to become legitimate purchases, its effects should be stronger for heavily pirated music than it is for other music genres.

Keywords: *Piracy, regulation, digital distribution, music industry, natural experiment.*

I. Introduction:

Since the rise of Napster, "piracy killed the radio star" could be the global slogan of the music industry. Global recorded music sales and licensing have plunged from nearly $27 billion US dollars in 2000 to $15 billion in 2010,[1] with some countries witnessing a coinciding decrease in investment in developing local talent (IFPI 2010). An increasingly popular topic in the economics and the information systems literatures has been how much of this sales decrease is due to displacement by Internet piracy. While estimates vary, the vast majority of studies find that piracy has caused a significant decrease in music sales (see for example, Liebowitz (2006), Rob and Waldfogel (2006), Zentner (2006), Hui and Png (2003), OECD (2009)). However, to date there have been far fewer academic studies analyzing whether anti-piracy measures can mitigate some of the sales loss from piracy — and none that we are aware of that are directly related to governmental intervention. Our goal in this paper is to provide such evidence, by evaluating the effectiveness of anti-piracy government intervention in France.

Since the rise of Napster in 2000, media companies have pleaded with governments worldwide to consider newer, more creative anti-piracy laws and strategies to mitigate the impact of piracy on sales. In May of 2009 the French Parliament passed an anti-piracy law known as HADOPI, or the Creation and Internet Law. The purpose of this law is to "promote the distribution and protection of creative works on the Internet." The law empowers the HADOPI administrative authority to send warnings to identified infringers and transfer the case to the court in cases of repeat infringement. HADOPI acts on the basis of information submitted by rightholders and has the power to monitor online infringement and verify information with ISPs. When a rightsholder submits a notice of infringement, it is verified by HADOPI and matched against information held by the relevant ISP. Valid infringement triggers a notice of infringement sent by email from HADOPI to the account holder. When the same account is identified again as being used for infringement within a period of six months of the first warning, a second warning

[1] Source: IFPI. This includes both digital and physical sales of recorded music.

is sent by HADOPI to the account holder, this time by registered mail. Where the account is identified for a third time within a period of one year, HADOPI may escalate the case by referring it to the criminal court, where a judge is empowered to order a range of penalties, including account suspension for up to one month.[2] This law has been controversial on several major fronts, including the cost of the law, suggestions that Internet access may be a human right, potential violations of the principle of net neutrality, and the possibility that the law could hold Internet users responsible for copyright violations even if their computers have been hijacked.

The purpose of this study is not to debate the broader social and policy merits of this law. Instead, our purpose is to analyze whether this law had an impact on consumer behavior. This question is important for two reasons. First, music industry profits are clearly important to individuals working in that industry. Second, a broader social concern is that if the media industries are less able to recoup profits on their investments in creative works they will likely decrease their investment in bringing new music, television, and films to society, thus reducing overall social welfare.

In this regard, we evaluate the effectiveness of HADOPI using a panel of iTunes sales data for the four major music labels (Universal Music, Warner Music, EMI Music and Sony Music) across a broad set of countries.[3] We employ a difference-in-difference approach, using sales trends in selected European countries to simulate the counterfactual of what music sales in France would have been if HADOPI had not been passed. Using Google Trends, we find that public awareness of HADOPI became widespread in Spring 2009, and our difference-in-difference model suggests that HADOPI awareness caused a 22.5% increase in iTunes song unit sales in France (over and above any change in the control group), as well as a 25% increase in iTunes album unit sales (over and above the change in the control group). Closer

[2] See the HADOPI law itself in articles L 331-25 and L 336-2. Or an explanatory memorandum from the French government at http://www.culture.gouv.fr/culture/actualites/conferen/albanel/creainterenglish.pdf.

[3] We study digital sales for two reasons: first, the data are more readily quantifiable than physical sales are (unlike with digital sales, there are no comprehensive sources of physical sales data). Second, previous studies have shown that illegal Internet downloaders prefer digital sales channels over physical ones when purchasing legally. For example, see Danaher et al. (2010).

examination reveals similar trends separately for each of the four major music labels, suggesting that our industry-wide results are not driven by one label's advertising campaign or marketing activity.

To test the validity of our results, we add another level of difference to the model. Previous research and new survey data reveal that music genres differ in their tendency to be pirated. One would expect that if the observed relative increase in French sales is caused by HADOPI, that high-piracy genres would experience a larger increase in sales than low-piracy genres do. Our results are consistent with this hypothesis: low piracy genres experienced only a 7% difference-in-difference sales increase in France after HADOPI, while high piracy genres experienced a 30% difference-in-difference increase in sales, a result that is consistent with the hypothesis that the observed increase in French sales after HADOPI is due to a reduction in Internet piracy.

II. Background on Music Industry and HADOPI

Looking at aggregate sales reports it's easy to see why the music industry might be concerned about the impact of piracy on sales. Forrester research and the Recording Industry Association of American (RIAA) have reported that music industry revenue in the United States dropped by 46% from $14.6 billion in 1999 to $7.7 billion in 2009.[4] Worldwide sales have seen a similar drop of 44% from $27 billion in 2000 to $15 billion in 2010. Studies by the IFPI have found corresponding decreases in investment in local talent in some countries. However, the economic literature is only just beginning to address the question of whether diminished music industry returns due to piracy cause a decrease in the amount of creative works brought to the market.[5] Nonetheless, academic studies on the effect of piracy suggest that online file sharing can explain anywhere from one fifth to all of the decrease in music industry revenues since

[4] http://www.riaa.com/faq.php
[5] See, for example, Oberholzer-Gee and Strumpf 2009 or Waldfogel 2011.

2000,[6] and because of this it is important to understand what sorts of policies or strategies can act to mitigate this negative impact.

In June 2008 the HADOPI Law was first presented to the French Senate by several politicians, and in October 2008 the Senate backed the law, meaning that it would next go before the French National Assembly. (However, as we will show in more detail below, there was relatively low publicity around the law or national awareness of it during this time). In March 2009 the HADOPI law was presented to the National Assembly, where it was at first supported and then rejected in 2009. This debate gave rise to a number of media articles generating awareness and controversy.[7] Importantly, this could have led to some confusion among the general populace over whether the law was yet effective or not. In May 2009 both the National Assembly and the Senate backed an amended version of the law, leading opposition Parliamentarians to send it to the French Constitutional Council for review. In June 2009 the Constitutional Council rejected the main part of the law (again potentially adding to confusion over whether the law was yet in effect), largely over the issue of judicial review for penalties imposed by the third strike (in this early version of the law, penalties could be applied to individuals on the third infringement without judicial review). This section was then amended to require judicial review, and the Constitutional Council accepted the amended law in October 2009, putting the law into effect.[8]

From that point onward, filesharers in France could theoretically begin to receive notices of infringement. However, it was over a year before the HADOPI agency began sending out first notices, with the first wave of infringement notices going out in September 2010. Later, in Spring 2011, the HADOPI agency began the initial wave of second notices, and as of August 2011 no third notices had been sent out and no penalties had yet been applied.[9]

---

[6] See the music piracy studies cited in our literature review.
[7] For example, http://news.bbc.co.uk/2/hi/europe/7992262.stm
[8] For references regarding the political timeline of the HADOPI law, see law http://www.senat.fr/dossier-legislatif/pjl07-405.html and http://www.conseil-constitutionnel.fr/decision.42666.html.
[9] This timeline is outlined in a short report titled "Hadopi, cultural property and Internet usage: French Internet users' habits and points of view" available at http://www.hadopi.fr.

It is also important to note that while the most publicized responsibility of the HADOPI agency under the law is to send out infringement notices, as part of the HADOPI legislation the agency started an education campaign to inform citizens about the illegality of sharing copyrighted materials online, the dangers it may pose to content generation in the future, and the various legal channels in which media can be obtained. These campaigns are an ongoing part of HADOPI's responsibilities. Unfortunately (from a research perspective), these campaigns are ongoing and do not represent discrete events. Thus their effects cannot be separated from the effects of the graduated response/penalty portion of the law, and our study must be about the combined effect of both these education campaigns and the warning and penalty system.

III. Literature Review

Our research is most closely related to the large literature analyzing how piracy has impacted media sales. This literature has used a variety of empirical methods from cross-country or cross-city variation in piracy levels (e.g., Zentner 2005, Hui and Png 2003, Peitz and Waelbroeck 2004, Liebowitz 2008, and Danaher and Waldfogel 2011) to survey data (e.g., Rob and Waldfogel 2006, Rob and Waldfogel 2007) to exogeneous shocks in the availability of pirated or legitimate content (e.g., Oberholzer-Gee and Strumpf 2007, Smith and Telang 2009, Danaher et al. 2010). What this literature has in common is that nearly all of the academic studies find that media piracy has a significant negative impact on sales. The one exception to this rule, Oberholzer-Gee and Strumpf 2007, is also one of the earliest studies of piracy's impact, and has seen some concerns expressed about its findings in recent years (see Liebowitz 2008, Liebowitz 2011).

Our research is also closely related to a smaller literature on the impact of anti-piracy intervention on sales and the availability of pirated content. In this literature Bhattacharjee et al. (2008) analyze how the RIAA's legal threats against file sharers impacted sales. The authors treat the industry's legal intervention (and associated press coverage) in 2003 as a quasi-experiment, and find that the lawsuits had a

statistically significant negative impact on the availability of pirated content, but that a substantial amount of illegal content was still available even after several highly publicized lawsuits against filesharers. Notably, however, this study did not address the impact of the lawsuits on sales.

In the context of the use of DRM, Desai et. al. (2009) and Sinha et al. (2010) argue that the use of DRM may *increase* piracy by making the content less usable for end-users. Similarly, Kemerer, Liu, and Smith (2011) argue that the use of DRM may make it more likely that a single dominant platform will emerge in digital media sales channels — potentially creating powerful downstream players, such as iTunes, for the industry to negotiate with. Finally, in the computer science literature Christin et al. (2005) have analyzed the effectiveness of file sharing "poisoning" strategies, finding that a few intentional decoys of pirated content can influence perceived availability of content in the networks.

Lastly, our study relates to a growing literature analyzing the impact of digital sales channels on sales in physical channels and on piracy. In this literature, Deleersnyder et al. (2002) show that the availability of digital news in England and the Netherlands has only a small impact of readership in physical channels. In the context of video distribution, Waldfogel (2009) uses survey data to find that YouTube viewing of television content has almost no impact of television viewership levels. Likewise, Danaher et al. 2010 find that iTunes distribution of television content has no statistical impact on sales of DVD box sets of that content, but a large negative impact on piracy levels. Finally, Hu and Smith (2011) find that the distribution of Kindle ebooks has a very low impact on sales of print books.

IV. Theory

Our main theory of the impact of HADOPI is closely tied to the original intent of the law: HADOPI may cause consumers who otherwise would have pirated music to avoid piracy, and some of these consumers may instead purchase music through legitimate channels. There are, however, two important theoretical questions about the impact of the law that warrant discussion. First, when should we expect the impact of

the HADOPI law? Will it occur primarily around national awareness of the law, or when the law actually goes into effect? Second, will HADOPI cause increased consumption of legal music and will this consumption occur in digital or physical channels?

With respect to the second question, as noted above, the literature seems to suggest that consumers are strongly tied to either the digital or physical channel such that if a consumer is forced to stop consuming digital piracy, the literature suggests that they are more likely to switch to other digital channels than they are to return to CD purchases (see, for example, Danaher et al. 2010, Hu and Smith 2011). Because of this, we focus on the impact of HADOPI on digital music sales,[10] reflecting our belief that if HADOPI impacts individuals' ability to pirate online, they are more likely to turn to digital music channels than they are to go back to physical purchases of CDs.

However, since nearly all prior papers in the literature indicate that filesharing displaces sales of physical music, it is a limitation of this paper that we are only able to examine iTunes sales data as it is possible that HADOPI could affect physical sales in addition to digital sales. Unfortunately, physical retail sales data were not available to us at the time of this study. Our data also do not reflect revenues from newer legal music streaming platforms such as Spotify or Youtube channels, and we discuss this limitation further in the conclusion if this paper. Thus, our study asks the question of whether a law like HADOPI can stimulate sales of one form of media (music) in one channel (iTunes), and as such likely does not capture the total impact of the law.

With respect to the first question, there is no strong theoretical basis in the literature for whether HADOPI's impact will begin primarily when the public becomes aware of the law or with the actual dates of passage, legal notifications, and legal penalties. Many economic studies of policy changes focus on the date of passage of the new policy as the treatment date. However, because HADOPI went through a significant public and political debate before being passed, and because citizens may not have even been

[10] Data from the Syndicat National de L'edition Phonographique (SNEP) indicate that 20% of French music sales in the first 3 quarters of 2011 were digital, with physical making up the remainder (http://www.disqueenfrance.com/fr/catalogpage.xml?id=420906&pg=1&cat=251362).

aware of the actual effective date of the law, we believe it possible that public awareness and salience of the law could drive a change in behavior before it actually became effective. Lacking a strong theoretical basis, in our analysis below we test for both effects, finding a stronger impact around the peak awareness of HADOPI than from the specific passage of the law or the dates associated with first notifications of violations. Notably, some research in the criminology literature suggests that a policy change (such as an announced police crackdown on crime) may have an impact on behavior prior to actual enforcement of the policy, particularly when there is uncertainty among offenders of the timing of enforcement or the probability of being caught (Sherman 1990).

V. Data

For this study, we obtained a panel of total weekly iTunes sales units for a number of European countries including France. Our data extend from July 2008 to May 2011, and we observe separately both track unit sales and album unit sales. The data were obtained directly from the four major music labels — EMI, Sony, Universal, and Warner — and aggregated to reflect total iTunes sales for the majors. According to the IFPI, the four majors reflect roughly 70% of music industry sales, with independent labels reflecting the other 30% not observed in our data. We chose the five European countries (other than France) with the highest iTunes sales levels as our control group for France, under the theory that overall market trends would have the most similar impact on countries with closer sales levels.[11] Thus, in this study we observe weekly iTunes sales units for France, the UK, Italy, Spain, Germany, and Belgium. This yields 918 country-by-week observations of total iTunes sales units, broken down into albums and tracks.

We also have a separate dataset provided to us by just two of the four major labels. This dataset is similar to the dataset above except that for each country-week, we observe total iTunes song sales units for each genre of music. We use this dataset as a further test of our main effect, focusing on the following genres:

[11] However, any results reported in this paper are not sensitive to this selection of control group. Results remain roughly the same (and completely the same in sign and significance) when choosing a variety of other control groups).

Rap, Hip Hop, Rock, Pop, Classical, Christian, Folk, and Jazz. Our purpose in choosing these genres was to keep only genres which had a significant share of the market and for which we had reasonable priors regarding relative piracy levels for the genre.[12]

Table 1 shows the average sales levels per week (both track and album) across each of the countries as well as providing some indicators of the level of variance within each country.

Table 1: Descriptive Statistics

	iTunes track unit sales (thousands)			*iTunes album unit sales (thousands)*		
Country	**Mean**	**Median**	**Std. Dev.**	**Mean**	**Median**	**Std. Dev.**
Belgium	133.4	130.1	21.3	9.8	9.7	2.2
Germany	728.1	691.6	148.9	87.4	85.0	22.9
Spain	65.7	64.1	11.6	10.1	9.8	2.3
France	447.7	473.9	96.6	49.7	53.4	14.7
Italy	183.9	187.7	37.1	18.7	18.6	4.6
UK	2899.3	2801.9	594.0	270.7	275.2	82.7
Total	743.0	252.6	1022.3	74.4	25.9	98.6

The UK is clearly the largest country in terms of iTunes sales, and Spain is the smallest. We note from Table 1 that while there is significant variance across countries in terms of sales levels, the variance within countries (across weeks) is relatively smaller and less skewed. In spite of the variance in sales across countries, we will show that the average time trend of our control group — on a logarithmic scale — closely maps the time trend of France.

Finally, we postulate that because citizens may be confused over when the law actually became effective, we may be more likely to see an effect begin when people first became aware of the law rather than when it finally became effective in October 2009. To measure awareness, we collected Google Trends data on

[12] For example, we dropped the Country genre not because its market share was too low, but rather because we could find no research or data giving us information as to its a priori tendency to be pirated.

Google searches (from France) for the search term "HADOPI."[13] Google Trends reports the "relative search index" for a search term in a given country, meaning that for each week we observe the number of searches for that term relative to the average number of all searches in that country across each week in the date range. So, for example, if there were an average of 20,000 searches per week in our date range for the term HADOPI, then in a week where there were 100,000 searches, the Google Trends index would report "5.0" for that week. Thus, while we do not know the actual volume of searches, we know when awareness of HADOPI peaked as measured by Google searches, and the relative height of that peak. This can serve as a measure of national awareness of the law.

VI. Results

Our basic strategy for determining the impact of HADOPI is to use a difference-in-difference approach, comparing the change in French sales before and after HADOPI to the average change in sales across the control group. However, we have two initial challenges to overcome. First, we need to give evidence that our control group truly can simulate the counterfactual of what France's sales would look like in the absence of HADOPI. Second, we need to determine the appropriate "treatment date" on which HADOPI began.

We begin addressing both of these issues with the following model:

$$\ln Sales_{it} = \beta_0 + \beta_1 \Omega_t + \beta_2 \Omega_t * France_i + \mu_i + e_{it} \qquad (i)$$

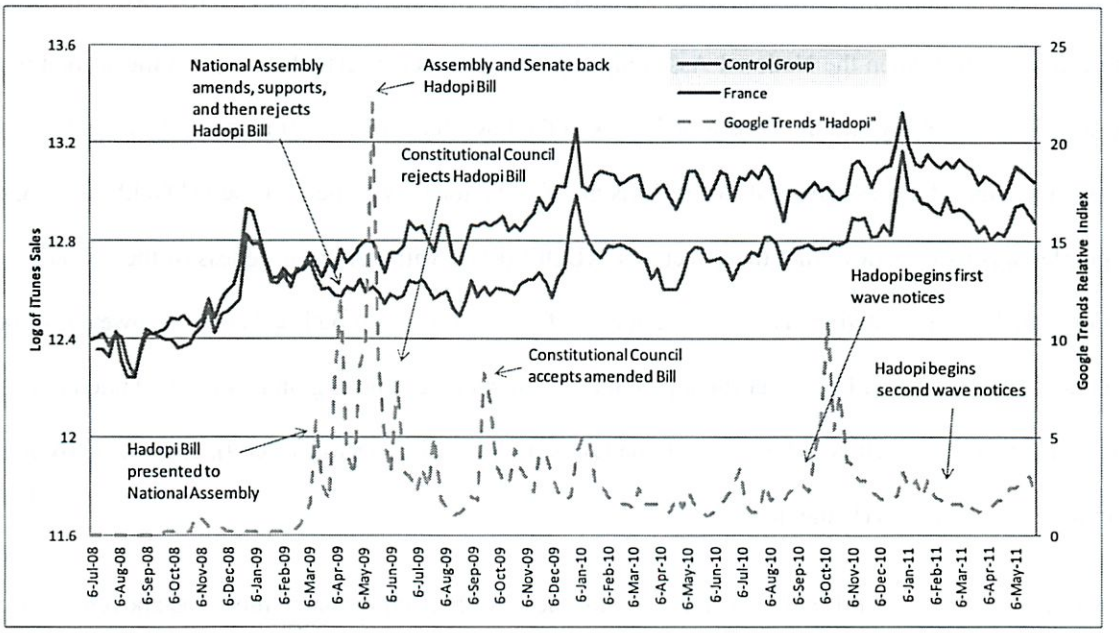
Where $\ln(sales_{it})$ is equal to the natural log of song sales units in country i during week t, Ω_t is a vector of dummy variables for each week of the data (time fixed effects), $France_i$ is an indicator variable equal to 1 for French observations, μ_i is a vector of country fixed effects, and e_{it} is the idiosyncratic shock term.

[13] Google Trends data for other related search terms such as "French Three Strikes Law" show the same pattern.

With this specification, β_1 tracks the average time trend for log sales units over time for the control group, while β_2 estimates how the French time trend differs from this average.

We estimate this model and then plot the results visually in Figure 1, with $\beta_0 + \beta_1$ representing the average sales time trend for the control countries and $\beta_0 + \beta_1 + \beta_2$ representing the French sales time trend. Both of these time trends are plotted and measured on the left axis in Figure 1. We also added to this graph the Google Trends relative index for the search term HADOPI (in France), measured on the right axis.

Figure 1: iTunes Single Track Unit Sales Trends (4 majors combined), France vs. Control



Examining this table, we first note that the initial peak for the Google Trends Index occurs in March 2009, corresponding to the presentation of the HADOPI law to the National Assembly. Prior to March 2009, the French sales trend appears to follow closely the sales trend of the control group. A Wald test of joint significance for all β_2 between July 6, 2008 and March 30, 2009 could not reject the null hypothesis

that the coefficients are jointly zero at the 95% confidence level.[14] Thus, prior to the first Google Trends spike, the time trend for French sales is statistically indistinguishable from the sales trend of the control group. This lends credibility to the identifying assumption of our difference-in-difference model, namely that the control group simulates the counterfactual of how France's sales would have trended in the absence of HADOPI.

Figure 1 also helps to shed light on the question of when to consider the effective treatment date of HADOPI. The final HADOPI law that was passed was not accepted by the Constitutional Council until October 2009, and thus before this date the law was not actually in effect. However, we see the French sales trend diverge from the control group starting in March 2009, and then rise further throughout the following several months. During this time, we also observe two more peaks of HADOPI awareness; the first occurs in April when the National Assembly supports and then rejects the law, and the second is in May when the Assembly and the Senate both backed the law. Because each of these peaks is higher than the last, it seems safe to assume that this reflects growing national awareness of the HADOPI law. Thus, this graph leads us to believe that the effect of HADOPI began with rising awareness of the law and not upon its actual implementation. This seems plausible for the reasons we outlined above. However, in our subsequent analysis we will consider three potential treatment dates: the beginning of media attention and national awareness (March 2009), the month the law went into effect (October 2009), and when HADOPI began to send out notices (September 2010).

We also note a very similar trend for iTunes album sales. We applied the same model as above to iTunes album unit sales and graph the results in Figure 2.

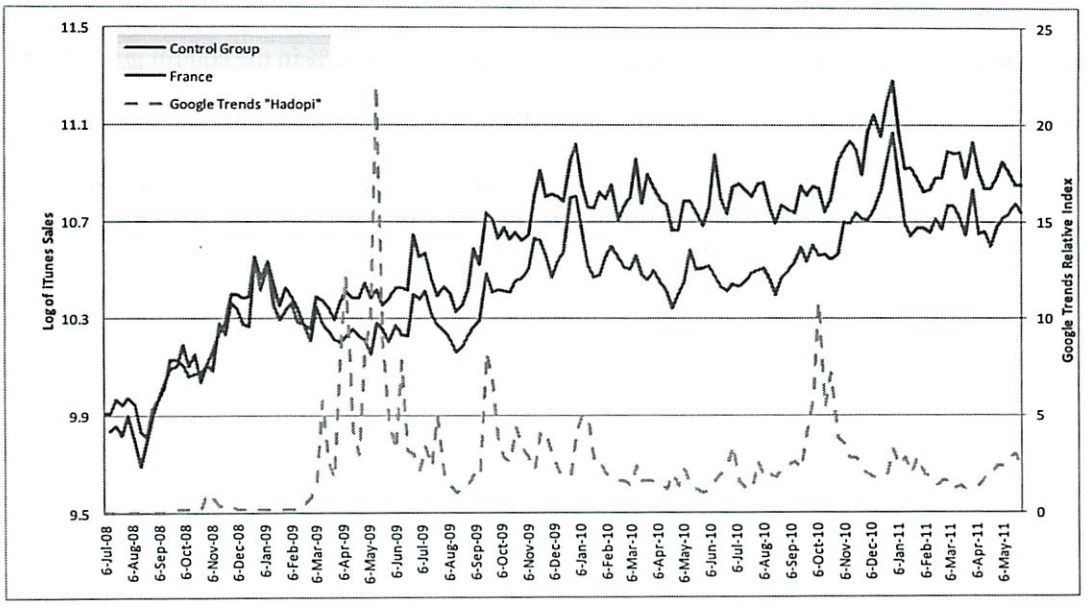
If we accept the identifying assumption that France would have followed the sales trend of the control group if not for HADOPI, then the average effect of HADOPI can be measured as the average gap

[14] We clustered standard errors at the country level, as observations of sales levels within a country from week to week are likely to be correlated.

between the two sales trend lines after March 30, 2009[15] (or, whichever date we are testing as a potential treatment date). In order to measure this gap and test for statistical significance, we estimate the following slightly different version of the first model:

$$\ln Sales_{it} = \beta_0 + \beta_1 \phi_t + \beta_2 \phi_t * France_i + \mu_i + e_{it} \qquad (ii)$$

Figure 2: iTunes Album Unit Sales Trends (4 majors combined), France vs. Control



The only difference between (ii) and (i) is that in (ii), ϕ_t is an indicator variable equal to one if the observation occurs after March 30, 2009 (or October 31, 2009 and September 30, 2010 in our sensitivity tests below). Thus, this model measures the average post-HADOPI change in sales across the control countries (β_1) and then estimates any change in French sales over and above the change in the control group (β_2). This means that β_2 is the coefficient of interest and under our identifying assumptions, it

[15] We note that the use of March 30, 2009 as the treatment date will likely yield a slightly conservative estimate of the impact of HADOPI. In Figure 1, it appears as if French sales may have begun to diverge from the control group during March and that the awareness of the law began to spike in early March, and so our conservative use of March 30 as the start date of HADOPI will bias our difference-in-difference estimate slightly toward zero.

represents the average causal effect of HADOPI on weekly iTunes sales units in France from March 2009 until May 2011.

In columns (i) and (ii) of Table 2 we display the results of estimating this model for both single tracks and for albums. Accounting for the fact that our independent variable is in log terms, these estimates indicate that iTunes track sales units rose about 25.5% in the control group after March 1, 2009 but by 48% in France, indicating that French iTunes track sales were 22.5% higher on average than they would have been in the absence of HADOPI.[16] Similarly, album sales units rose by 42% in the control group but 67% in France, indicating that HADOPI increased iTunes album sales an average 25% per week in France. Standard errors are clustered at the country level, and these difference-in-difference results are statistically significant at the 95% confidence level.[17]

[16] Additionally, we estimated this model for the 6 months before and after the month the law became effective (October 2009) since fully informed, rational consumers need not change their behavior until then. The coefficient of interest is smaller in this specification and significant only at a 90% confidence level. We also estimated the model for the 6 months before and after September 2010, as this was the first month that HADOPI began sending out first notices. In this case, the resulting coefficient was close to zero and statistically insignificant. We suggest that consumers likely reacted more to the media attention in March-May 2009 both due to its salience and because it may have been unclear to them when the law actually became effective.

[17] There has been some recent criticism of standard methods for clustering standard errors in difference-in-difference models when the number of groups is small. See, for example, Bertrand (2003). We also collapsed the data into 12 observations, summing up track sales for each country before and after March 30. When we estimate the model on these 12 observations, the coefficient of interest (the France-after interaction) is still estimated as 0.2 and is still significant at the 95% confidence level.

Table 2: Estimate Effects of HADOPI for Tracks, Albums, and Across Genres

	(i)	(ii)	(iii)	(iv)	(v)
	All Tracks	All Albums	Classical / Folk / Modern Christian / Jazz	Rock / Pop	Rap / Hip Hop
After Hadopi	0.228*	0.351*	-0.042	0.142	0.846*
	(0.037)	(0.033)	(0.072)	(0.068)	(0.205)
After Hadopi * France	0.203*	0.223*	0.068	0.158**	0.260
	(0.037)	(0.033)	(0.072)	(0.068)	(0.205)
Constant	12.520*	10.168*	7.715*	11.411*	8.731*
	(0.023)	(0.020)	(0.044)	(0.042)	(0.127)
Observations	918	918	912	912	912
# of Countries	6	6	6	6	6
R-squared	0.361	0.417	0.082	0.103	0.42

Robust standard errors in parentheses
+ significant at 10%; ** significant at 5%; * significant at 1%
March 30, 2009 is counted as the beginning of Hadopi
Columns (i) and (ii) include data from all four majors, while columns (iii) through (v) reflect data from only two.

In addition to these aggregate results, we also estimated the same models for each of the four major labels individually, and the results for each individual label exhibit roughly the same patterns as the aggregated results (particularly in sign and significance). Thus, it is unlikely that our results are driven by the marketing efforts or release schedule of an individual firm. As well, marketing, advertising, and release schedule decisions must — by law — be made non-cooperatively, making it less likely that they will be correlated across labels. In short, the effects we have observed thus far appear to be industry-wide and not specific to any particular label's music.

We also conducted a series of placebo tests. We ran the same difference-in-difference model five more times, each time supposing one of the countries in our control group to be the "treatment" country. We were unable to reject the null hypothesis for any country in these tests; in other words, for each country (other than France) we cannot reject the hypothesis that that country's sales increased by no more than the average of the other countries. Thus, at least with regard to the countries we studied, our findings are unique to France.

Genre Analysis

Policy changes such as these are often difficult to study due to a lack of experimental power. Indeed, although we observe five control countries over time, we only observe one experiment: the passage of HADOPI in France. One could argue that some other French-specific factor may have coincidentally affected France's music sales levels at exactly the same time as public awareness of HADOPI. While we believe that it is unlikely that the timing of this would coincide with the passing and awareness of HADOPI, we cannot rule out this possibility based on the preceding tests.

In an attempt to partially address this concern we add an additional level of difference to the model based on priors about the popularity of piracy across various genres of music. Specifically, EMI surveys of French citizens show that that Rap and Hip Hop are the most heavily pirated genres, even relative to popularity in legal sales channels. While Rock and Pop experience average levels of piracy, the data also indicate that genres such as Classical, Christian, Folk, and Jazz experience significantly lower levels of piracy.[18] We also note that other published studies suggest a similar distribution of pirated downloads across genres.[19] This allows us to increase the number of experiments in that we can treat each genre as a unique experiment based on its *a priori* tendency to be pirated. If the observed increase in French sales is due to a reduction in piracy triggered by HADOPI, we would expect the increase in Rap sales to be larger than that for Rock and Pop and the increase for Classical, Christian, etc. to be quite low.

In columns (iii), (iv), and (v) of Figure 2 we see that that the rise in French sales after HADOPI (relative to the control) is indeed highest for the most heavily pirated genres (column v) and is small and statistically insignificant for the least pirated genres (column iii). We conducted an F-test across each estimation to test whether the estimate of the effect of HADOPI on French sales is different across genres. Due to relatively large standard errors for Rap and Hip Hop, while the point estimate on Rap and Hip Hop

[18] These genre findings are based on surveys performed by EMI Music in France during October and November 2010. 8,173 interviews were completed and results were weighted to nationally representative figures. The data are not publicly available but were available to the authors.
[19] For example, Liebowitz (2008).

is larger than either Rock/Pop or Classical, Folk, Christian, and Jazz,, we cannot reject the null hypothesis the post HADOPI French increase in rap/hip hop is the same as for the other genres. However, we can reject with 90% confidence the null hypothesis that the French increase (above the control group) in Rock/Pop is the same as for less pirated genres like Classical and Jazz. Nonetheless, the point estimates indicate that that while the effect of HADOPI increased iTunes sales of Classical, Christian, Folk, and Jazz genres in France by 7%, the point estimate of the effect on Rock and Pop was 17% and the effect on Rap and Hip Hop was 30%.

Unobserved changes that might increase French music sales (around the same time as HADOPI) would be unlikely to have this same pattern across genres. For example, if Apple began to heavily promote the iTunes store in France more so than in the control countries around the same time as HADOPI, one would expect such promotions to affect each genre equally, at least proportionally to prior sales. Instead, we see sales in France for heavily pirated genres rise faster than for less pirated genres, which suggests that this sales increase is due to a reduction in French piracy levels. This is consistent with the idea that the difference-in-difference increase we observe in France is actually attributable to HADOPI.

Challenges to Identification

In this study, causal inference rests on the assumption that sales of the control group would have trended similarly over time to French sales in the absence of HADOPI. Indeed, the time trend for French sales is statistically indistinguishable from the control group's time trend prior to HADOPI. However, it is possible that conditions in France may have changed differentially from the control group, leading us to observe an increase in French sales and falsely attribute it to HADOPI. In this regard, any phenomenon "X" that would have led to the trends we observed in the data would have to meet two conditions: First, it must be true that X began to change differentially in France relative to the control around March/April of 2009, and that X would have an impact on iTunes sales. If a phenomenon X occurred at some other time — say, June 2010 — then it is unlikely to explain the pattern we observe in our data, as sales in France

began to increase relative to the control countries in March 2009, and in June 2010 French iTunes sales do not appear to trend differently than the control group. Second, X would have to have a stronger effect on Rap/Hip hop sales, and a weaker effect on Jazz/Classical/Christian/Folk sales, than on sales of other genres. For example, if Apple coincidentally began a general iTunes marketing campaign in France in March 2009 (and did not do so in the control countries), this still would be unlikely to explain our observations unless the marketing campaign were primarily directed toward audiences of heavily pirated genres.[20]

One phenomenon that might meet these criteria would be French adoption of devices connecting to the iTunes music store. For example, if sales of mobile iOS devices in France diverge substantially from sales in the control group countries starting with HADOPI, this in turn might affect iTunes sales, undermining our results.[21] In Appendix I we address this possibility and show that the French adoption rate of iOS mobile devices (devices that connect to the iTunes store) was no higher during this period than it was for the control countries.

VII. Discussion

Combined, the four major labels sold an average of 491,000 tracks per week in France after March 2009. Our findings suggest that in the absence of HADOPI, if France followed the same trend as the control group,[22] sales would have averaged only 401,000 units per week. Thus, our results suggest that the HADOPI law (and the education and media attention surrounding it) increased iTunes single sales by 90,000 units per week on average. If we assume an average song price of €1 per song, this equates to an increase of €4.7 million ($6.3 million) in annual iTunes track revenues.

---

[20] We note that we are aware of no Apple campaign during this timeframe that was specific to France.

[21] We note that even in this scenario, the increase in iOS device may be related to HADOPI if HADOPI causes consumers to be more likely to purchase from iTunes and purchasing from iTunes causes consumers to be more likely to purchase iOS devices. Thus, even if sale of iOS devices substantially increased in France around HADOPI, it may not necessarily undermine our estimates. However, as we show in the Appendix, there is no evidence that the uptake of these devices was different in France during this time period.

[22] Which they did for the period of time from July 2008 until March 2009.

Likewise, average iTunes album sales were about 56,000 units per week in France after March 2009. In the absence of HADOPI, we estimate that iTunes album sales would have averaged only 44,800 albums per week. Thus, our results suggest that HADOPI causally increased French digital albums sales by an average of 11,200 units per week. Assuming an average of €8.5 per album, this equates to an increase of €4.9 million ($6.7 million) in annual iTunes album sales due to HADOPI. Together, our estimates suggest that HADOPI increased annual iTunes revenues (tracks plus albums) by about €9.6 million ($13 million) per year for the four majors combined.[23] Under the assumption that the four majors make up 70% of the industry, if sales for the remaining 30% of artists experienced the same change in sales as we observe for the major labels, then the impact of HADOPI was to increase overall digital iTunes sales by €13.8 million ($18.6 million) per year for the entire music industry.

We also note that the effect of HADOPI was larger for more heavily pirated genres like Rap and smaller for less pirated genres like Christian music or Jazz, which is what one would expect if the increase in sales were causally related to HADOPI. It is also worth noting we observed this sales pattern for each of the four majors when analyzed separately, providing some support our assumption that HADOPI may have had a similar effect on the independent labels (the other 30% of the market). Finally, we note that our results do not appear to be explained by an increase in Apple iOS devices in France relative to the control group countries.

The most interesting, and potentially surprising, part of this conclusion is that the study occurs before anyone received a third notice (i.e. before any cases have been referred to the criminal court), and that the increase in sales is observed even before the law's final passage. While this may seem irrational, it is consistent with the idea that increasing the salience of the law, the illegality of piracy, and the potential penalties is sufficient to change user behavior. In this regard, we note the significant discussion in the media about the illegality of piracy while the law was being debated, and that after the passing of the law,

[23] According to sources inside the major labels, about 30% of this goes to iTunes while the other 70% is split in some manner between the label and the artist.

the HADOPI agency has also conducted extensive awareness and education campaigns about the illegality of media piracy and the legal alternatives that are available. Thus, we cannot determine to what degree the continued effectiveness of HADOPI is driven by the threat of sanctions, the media buzz, or the educational/awareness campaigns. Disentangling the effects of the positive reinforcement actions like education from the negative reinforcement actions like sanctions is a fruitful area for future research.

A finding that education and salience have a strong impact on user behavior is consistent with those of Bhattacharjee et al. (2008), who find that public awareness of a very small number of major lawsuits conducted by the RIAA against music file-sharers reduced national supply and demand for pirated content on P2P networks. However, unlike Bhattacharjee we do not find that the effect is necessarily short-lived. We suggest that with regard to mitigation of sales displacement by piracy, a national anti-piracy policy combined with educational efforts may be much more effective in the longer term than are a small number of high-profile lawsuits. However, more research is needed to conclusively show how the educational components of an anti-piracy law affect user behavior separately from the enforcement components of the law.

As noted above, a limitation of our study is that we only observe data for one industry (music), in one channel (iTunes). Thus the conclusions should be generalized with some caution. However, this also means that our study likely understates the true sales impact of HADOPI. Within the music industry, physical CD sales are still a large component of music industry revenues; and while data limitations prevented us from considering the effect of HADOPI on CD sales, CD sales may have also have benefitted from HADOPI (as other academic studies have shown that filesharing displaces physical CD sales).

HADOPI may have also benefitted other channels for distributing music. For example, during this time legal music streaming services have become popular in Europe. These services provide revenues to the music industry in several manners not measured by this study. It is entirely possible that illegal

downloaders who choose to quit pirating due to HADOPI might turn to legal streaming services (such as Deezer, MusicMe or YouTube), meaning that revenue from streaming and other digital music sales channels may have increased due to HADOPI as well. However, some of these services — such as Deezer — were adopted after the impact of HADOPI, leaving us with no pre-HADOPI period to study. As well, growth trends in these services seem to vary greatly across countries, making selection of a control group difficult at best.

In short, while we suspect that revenues from these or other similar music services may have benefitted from HADOPI, we are unable to evaluate this claim with the same rigor or precision that we could with iTunes sales. As such, we believe that the €13.8 ($18.6) million per year increase in French iTunes revenues suggested in our results should be taken as a lower bound on the total effect that HADOPI has had on music industry revenues.

Additionally, other industries may benefit from HADOPI. For example, to the degree that the motion picture and publishing industries suffer losses caused by filesharing, HADOPI may positively impact revenues in those industries. So our study does not quantify the entire effect of HADOPI on producer surplus in the media industries, but merely indicates that for one industry (music) in one channel (iTunes), the law appears to have had a large and statistically significant effect.

For policy-makers, our results may have important implications in other countries that are considering passing similar graduated response laws, as well as in France where a number of parties oppose the continued existence of the law. Likewise, our results may inform industry practice in some countries, like the United States, that have seen the voluntary agreement between the music industry and Internet Service Providers on the application of a graduated response system. Though of course, generalizing our finding to other settings and countries would require additional considerations unique to those settings.

In the context of ongoing policy debates, we also wish to point out two important limitations of our study. First, our results only address the impact of this legislation on industry revenue. Our study does not

address the costs of this or other anti-piracy interventions. These costs could accrue either through the direct costs of implementing and enforcing the legislation, or through indirect social costs and potential side-effects associated with implementing such anti-piracy legislation, and such costs should be balanced against potential benefits in any discussion of policy change. Second, we wish to point out that our results should be viewed only in the context of efforts to influence the demand-side of piracy (i.e., through educating and influencing consumer behavior). It is unclear whether efforts to influence the supply-side of piracy (such as site blocking envisioned in the Stop Online Piracy Act proposed in the United States) will be similarly effective in altering consumer behavior.

References:

Bertrand, M., E. Duflo, S. Mullainathan. 2004. How Much Should We Trust Differences in Differences Estimates. *The Quarterly Journal of Economics*, 2 249-275.

Bhattacharjee, S., R. Gopal, K. Lertwachara, J. Marsden. 2006. Impact of Legal Threats on Online Music Sharing Activity: An Analysis of Music Industry Legal Actions. *Journal of Law and Economics,* 49 91–114.

Christin, N., A. Weigend, J. Chuang. 2005. Content Availability, Pollution, and Poisoning in File Sharing Peer-to-Peer Networks. *Proceedings of the 6th ACM conference on Electronic commerce*, pp. 68-77.

Danaher B., S. Dhanasobhon, M.D. Smith, R. Telang. 2010. Converting Pirates Without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy. *Marketing Science,* 29(6) 1138-1151.

Danaher, B., J. Waldfogel. 2011. Reel Piracy: The Effect of Online Movie Piracy on Film Box Office Sales. Working Paper. Wellesley College. Boston, Massachusetts.

Deleersnyder, B., I. Geyskens, K. Gielens, M.G. Dekimpe. 2002. How Cannibalistic is the Internet Channel? A study of the newspaper industry in the United Kingdom and The Netherlands. *International Journal of Research in Marketing,* 19(4) 337-348.

Desai, P., D. Purohit, D. Venik. 2009. Downloadable Music Set Free: The Flip Side of DRM Protection. Working Paper, Fuqua School of Business, Duke University.

Hu, Y., M.D. Smith. 2011. The Impact of Ebook Distribution on Print Sales: Analysis of a Natural Experiment. Working Paper, Carnegie Mellon University, Pittsburgh, PA. (Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1966115.)

Hui, K., I. Png. 2003. Piracy and the Legitimate Demand for Recorded Music. *Contributions to Economic Analysis & Policy*, 2(1) Article 11.

IFPI. 2010. IFPI Response to Commission Green Paper on Creative and Cultural Industries. July 2010.

Kemerer, C., C. Liu, M.D. Smith. 2011. Strategies for Tomorrow's 'Winners-take-some' Digital Goods Markets. Working Paper, Carnegie Mellon University, Pittsburgh, PA. Available at http://www.pitt.edu/~ckemerer/Kemerer-Liu-Smith--Submitted.pdf.

Liebowitz, S. 2008. File-Sharing: Creative Destruction or just Plain Destruction? *Journal of Law and Economics*, 49 1-28.

Liebowtiz, S. 2008. Testing File-Sharing's Impact by Examining Record Sales in Cities. *Management Science,* 54(4) 852-859.

Liebowitz, S. 2011. The Metric is the Message: How much of the Decline in Sound Recording Sales is due to File-Sharing? Working Paper, University of Texas at Dallas.

Oberholzer, F., K. Strumpf. 2007. The Effect of File Sharing on Record Sales. An Empirical Analysis. *Journal of Political Economy,* 115(1) 1-42.

Oberholzer, F., K. Strumpf. 2009. Filesharing and Copyright. *NBER's Innovation Policy and the Economy Series*, volume 10. MIT Press.

OECD. 2009. Magnitude of Counterfeiting and Piracy of Tangible Products. November 2009.

Peitz, M, P. Waelbroeck. 2004. The Effect of Internet Piracy on Music Sales: Cross-Section Evidence. *Review of Economic Research on Copyright Issues*, 1(2) 71-79.

Rob, R., J. Waldfogel. 2006. Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students. *Journal of Law and Economics*, 49(1) 29-62.

Rob, R., J. Waldfogel. 2007. Piracy on the Silver Screen. *Journal of Industrial Economics*, 55(3) 379-393.

Sinha R.K., F.S. Machado, C. Sellman. 2010. Don't Think Twice, It's All Right: Music Piracy and Pricing in a DRM-Free Environment. *Journal of Marketing*, 74(2) 40-54.

Sherman, L. 1990. Police Crackdowns: Initial and Residual Deterrence. *Crime and Justice*, 12 1-48.

Smith, M.D., R. Telang. 2009. Competing with Free: The Impact of Movie Broadcasts on DVD Sales and Internet Piracy. *MIS Quarterly,* 33(2) 321-338.

Waldfogel, J. 2009. Lost on the web: Does web distribution stimulate or depress television viewing? Information Economics and Policy, 21(2), 158–168.

Waldfogel, J. 2011. Bye, Bye, Miss American Pie? The Supply of New Recorded Music Since Napster. NBER Working Paper No. 16882.

Zentner, A. 2006. Measuring the Effect of File Sharing on Music Purchases. *The Journal of Law and Economics*. 49 63–90.

Zentner, A. 2005. File Sharing and International Sales of Copyrighted Music: An Empirical Analysis with a Panel of Countries. *Topics in Economic Analysis & Policy*. 5(1) Article 21.

Appendix I: iOS Devices

As noted above, it is possible that our results are explained by other phenomena, however, these phenomena would need to affect French iTunes sales more than sales in the control group countries, would need to do so during the HADOPI timeframe, and would need to have a larger impact on heavily pirated music genres than on less pirated genres.

One possible explanation that would fit these characteristics is that iTunes sales are strongly correlated with the overall penetration of Apple iOS devices (i.e., iPhones, iPods, and iPads), and that the penetration of Apple iOS devices increased significantly more in France than in the control group countries during our study period (and that this change was unrelated to HADOPI and that these new iPhone users prefer heavily pirated music genres). In this section we analyze whether sales of iOS devices can explain our results in this way.

To do this, we obtained data from IHS Screen Digest documenting total active iOS devices (iPhones, iPads, and iPods) for each country in our sample for the years 2008, 2009, and 2010. Table 3 displays the total active iOS devices for each country in all three years.

Table 3: Total Active iOS Devices (in millions)

Country	2008	2009	2010	% increase from 2008 to 2009	% increase from 2008 to 2010
France	1.02	3.02	5.91	197%	481%
Control group avg.				200%	586%
Belgium	*0.09*	*0.25*	*0.75*	*194%*	*776%*
Germany	*0.96*	*2.43*	*5.17*	*153%*	*439%*
Italy	*0.71*	*1.6*	*2.96*	*125%*	*317%*
Spain	*0.33*	*1.72*	*3.93*	*416%*	*1076%*
UK	*2.1*	*4.45*	*8.87*	*113%*	*323%*

Includes iPads, iPods, and iPhones capable of accessing Apple's App Store.

As the table shows, while French adoption of iOS devices increased by 194% from 2008 to 2009 and by 481% from 2008 to 2010, adoption in the control group countries increased by 200% from 2008 to 2009 and by 586% from 2008 to 2010. Thus, if anything, the change in penetration of iOS devices was slightly smaller in France than in the control group countries, a fact inconsistent with the proposed counter explanation for our results.[24]

We also note that the increase in iOS penetration in our control group countries is driven by an unusually large increase in iOS penetration in Spain. On one hand because our main results measure changes in French iTunes sales relative to aggregate sales in the control group countries, the relatively large increase in iOS device sales in Spain does not by itself present a problem for our analysis so long as overall iOS penetration in the control group countries is not significantly smaller than changes in iOS penetration in France.

However, the large increase in iOS device penetration in Spain relative to the other control group countries also presents an opportunity to test whether changes in iOS device penetration is a significant driver of changes in overall iTunes sales. To do this, in Table 4 we report estimates for (ii), except that here we compare the change in iTunes sales in Spain to the control group (not including France), before and after HADOPI.

As above, we count March 30, 2009 as the beginning of HADOPI. We note that both track and album sales for the control group (UK, Italy, Belgium, Germany) were increasing during this time. However, in spite of much higher growth in iOS mobile device penetration in Spain than in France or the control

[24] We note that because our analysis measures the change in French iTunes sales on a percentage basis relative to the control group countries, percentage changes are the appropriate comparison point to use for whether changes in iOS device penetration can explain our results.

countries, iTunes track sales in Spain grew no faster than sales in the control group did, and album sales grew at a slower rate.[25]

Table 4: iTunes Sales Before and After HADOPI, Spain vs. Control Group

	(i)	(ii)
	All Tracks	**All Albums**
After Hadopi	0.223*	0.376*
	(0.047)	(0.026)
After Hadopi * Spain	0.027	-0.129*
	(0.047)	(0.026)
Constant	12.490*	10.134*
	(0.028)	(0.016)
Observations	765	765
# of Countries	5	5
R-squared	0.277	0.371

Robust standard errors in parentheses
+ significant at 10%; ** significant at 5%; * significant at 1%

Thus, we find no evidence that changes in iOS device penetration in France are driving our results. The increase in iOS device penetration in France was, if anything, lower in France relative to the control group countries during the 2008 to 2010 timeframe. Additionally, a comparison of iTunes sales in Spain to sales in the control group countries shows no obvious evidence that changes in iOS device sales are significantly driving changes in iTunes sales.

[25] This finding should not be seen as a test of whether changes in copyright policy in Spain that were enacted in 2011 had any impact. This tests only whether the change in Spanish iTunes sales after March 30, 2009 was greater than the change in the control group over the same period.

Read 10/23

The Metric is the Message: How much of the Decline in Sound Recording Sales is due to File-Sharing?

Stan J. Liebowitz

School of Management
University of Texas—Dallas

November 2011

Abstract: The file-sharing literature has focused mainly on whether file-sharing has decreased record sales, with less attention paid to the size of any decline. Although there is still some contention, most studies have concluded that file-sharing has decreased record sales. What has not been noted is that most estimates indicate that the file-sharing has caused the *entire* enormous decline in record sales that has occurred over the last decade. This heretofore hidden result is due to the lack of a consistent metric that would allow easy comparability across studies. The task of this paper is to provide such a metric, translate the results reported in the literature into that metric, and then summarizes the results from this exercise.

How much of the highly publicized decade-long decline in the sales of authorized sound recordings is due to file-sharing? Although it is generally accepted that a large majority of empirical studies have found that file-sharing has caused a decline in the sales of prerecorded music, it is difficult for someone reading this literature to find a useful summary of the empirical estimates of the decline caused by file-sharing that might provide an answer to this question. This difficulty is due, in large part, to the different metrics of sales decline used in these studies as well as their use of differing empirical methodologies, different time periods and different geographic regions.

Although several articles, such as Connolly and Krueger (2005), DeJean (2009), Liebowitz (2005), and Oberholzer-Gee and Strumpf (2009), offer lengthy literature reviews, most of them, as well as the many obligatory reviews that are contained in studies of file-sharing, are generally focused mainly or entirely on the sign of the results—i.e., whether file-sharing has a negative impact on the sales of sound recordings. That focus may have made sense when the debate was largely about whether file-sharing had any negative effect at all on the sales of sound recordings. Nevertheless, the size of the estimated piracy-induced declines is of interest in and of itself and should be of greater interest than the sign, in part because the size of a coefficient contains more information than its sign, and also because the policy implications of file-sharing are likely dependent on the size of the estimates.

The purposes of this paper are threefold. First, it is to show that differences in the metric chosen to report the effect of file-sharing lead to important differences in the information conveyed. Second, it is to identify a metric that directly informs legal and economic consideration of the consequences of file sharing regardless of the time period or the countries used in the analysis. The final goal is to convert the estimates found in the literature into this metric so as to provide a meaningful comparison of the estimated size of file-sharing's impact on record sales. The metric that I use for this comparison is defined as the share of the sales decline that is due to file sharing over some period of time.

As I show below, when the results of these studies are made comparable in this manner, the estimates from a majority of studies imply that that file-sharing has caused the *entire* decline in sound recording sales that has occurred since the ascendance of Napster.[1] I believe this finding is likely to surprise even those

---

[1] As documented in Liebowitz (2006), Napster was born in 1999, grew to prominence in 2000, and was shut down in 2001.

who have been keeping up with this literature, since the prevalence of this result seems not to have been previously noted.

I. Candidate Metrics

Most econometric examinations of the issue tend to perform a regression of the form:

$$(1)\ RS = a + bFS + \boldsymbol{cZ}$$

where RS stands for record sales, FS stands for file-sharing and **Z** is a vector of covariates that are thought to influence record sales.[2] These regressions can be run across geographic regions, individuals, or albums, at a moment in time or as a time-varying panel. The coefficient b, which would be negative if file-sharing decreases record sales, represents the extent to which a downloaded song or album replaces the sale of that song or album.

There are at least three potential metrics of a decline in sales that might be proposed.

The most common method of measuring the impact of file-sharing is to create an estimate of the size of the decline in sales that is caused by file-sharing and then form a ratio of this decline as a percentage of overall sales:

$$Metric\ 1 = Share\ of\ Sales \equiv \frac{(b \cdot \overline{FS})}{RS}$$

Although this is a natural measure and the one most commonly adopted by researchers in the field, it does not allow comparability with other studies using the same measure, in spite of the fact that it is easy to simply compare percentage changes as a matter of arithmetic. The problem with comparing these percentages is that they will change not only as the amount of file-sharing changes but also as the closeness of the substitutability between

---

[2] In most instances there is no direct measure of file-sharing. Instead, a proxy, such as Internet usage, is often used. This may overstate the impact of organized file-sharing because other uses of the Internet that might reduce record sales (such as exchanging music files using email) cannot be separated from the impact of programs allowing organized and anonymous file-sharing. The results for these studies should probably be understood either to include a wider aspect of sharing files than organized file-sharing systems, or else to indicate an estimated result that is biased upward. Using the Internet, particularly for other forms of entertainment, might also usurp a user's time that would otherwise be used listening to music, causing a different upward bias in the estimated impact of file-sharing, although Liebowitz (2008) has estimated this bias to be quite small.

Could also do BT traffic

originals and unauthorized copies, which is a function of the technology in use by consumers.[3] This means that the same degree of file-sharing by the same people at different points in time will have different values for metric 1. This metric will also vary across countries and populations, for the same reasons.

A second metric could be coefficient b from the above equation:

$$Metric\ 2 = "displacement\ rate" \equiv b$$

Rob and Waldfogel, in their 2006 article, are the only authors of whom I am aware that use this particular measure which they label as the "displacement rate." This metric looks at the share of downloaded music that replaces the sale of music ("We find that each album download reduces purchases by about .2 in our sample, although possibly by much more"[4]). The problem with this measure is that translating it into an actual decrease in sales requires knowing how large the illicit download market is relative to the legitimate market. So the .2 reduction found by Rob and Waldfogel (2006) would imply a 20% reduction in sales if the legitimate and illicit markets were the same size but would imply a 40% reduction if the illicit market were twice as large as the legitimate market.[5] The ratio of the sizes of the licit to the illicit market is likely to differ across countries and over time, increasing the complexity of comparisons. It is perhaps for this reason that this metric is so uncommon among the papers on file sharing.

The most striking statistics in the sound recording industry, post-Napster, is the enormous decline in sales, as indicated in Table 1. A common question asked by many industry analysts is the extent to which the current decade-long decline has been caused by file-sharing. Answering this question provides

---

[3] The substitutability between originals and copies depends on how easy it is for unauthorized mp3 files to be played on the same audio devices and in the same locations as the legitimate purchased music that was available on CDs. In the early days of file-sharing MP3 files could not be played on most audio systems and converting MP3 files into the WAV files found on CDs required a CD burner which many users did not yet own. Over time, CD and DVD players gained the ability to play MP3 files, CD burners became commonplace, and MP3 players, such as the iPod, became the centerpiece of home and auto audio systems although the timing differed by country. These advances in technology increasingly made illicit downloads better substitutes for purchased originals.

[4] This statement is taken from the abstract of Rob and Waldfogel (2006).

[5] Liebowitz (2006) discusses various estimates of the relative size of the illicit download market (FS) relative to the legitimate market (RS) and concludes that the estimates of relative size are wildly disparate and that many estimates of the illicit market indicate that it is considerably larger than the legitimate market.

the third candidate metric for the impact of file-sharing: the share of any given decline that is due to file-sharing. This can be represented as:

$$Metric\ 3 = Share\ of\ Loss \equiv \frac{(b \cdot \overline{FS})}{\Delta RS}$$

This third metric has the advantage of allowing comparisons over time and across regions. For example, as illicitly downloaded files become better substitutes for legitimate versions (because of the growth of MP3 players, say), both the decline in legitimate sales and the decline in sales due to file-sharing will become larger even if the amount of file-sharing were to remain constant. But if the only reason for the decline in sales were file-sharing, then Metric 3 will remain unchanged at a value of 1, indicating that the role of file-sharing in causing the decline has not changed. This is particularly useful in comparing the decline across countries which will experience different diffusions of technologies that influence the substitutability of illicit and legitimate files.

This metric has problems in specific circumstances, however. For example, file-sharing could be harming sales but sales could still be growing. In this case it would be very awkward and probably meaningless to try to use Metric 3 to compare the estimated impacts of file-sharing over time since it would not even be possible to define the share of the decline that was due to file-sharing if there was no decline in sales.[6]

Table 1 indicates the size of the decline in the U.S., in both units and real revenues and real revenues for the non-U.S. portion of the world (labeled "non-U.S."). [7] Fortunately, U.S. and worldwide record sales have fallen in an almost monotonic fashion since the appearance of Napster. Further, Liebowitz (2007) provides evidence that each of the top markets has experienced a severe decline in sales so that Metric 3 can be used for the markets that have been empirically examined by economists.

---

[6] One might generalize this to try to account for a decline from any trendline, not just zero. If the actual growth of sales fell below trend, then even with an increase in sales it would be reasonable to consider the deviation from trend as lost sales and we could then examine the fraction of lost sales, measured in this way, that is due to file sharing. However, because those lost sales are conjectural, I have not recommended that approach here. Nevertheless, as we will see below, it is not unreasonable to encounter an effect of file-sharing that exceeds 100% of the observed decline in legitimate sales, implying that an upward trendline would have continued if not for file-sharing.

[7] The U.S. data on unit sales come from the RIAA website. Revenue statistics, both for the U.S. and non-U.S., come from the IFPI document "2010 Recording Industry in Numbers." Values for the non-U.S. portion of the world are dominated by the dozen or so leading markets.

Table 1: Decline in sales after the birth of organized file-sharing			
	U.S. Units	U.S. Real Rev	non-U.S. Real Rev
2000	4.8%	5.0%	4.3%
2001	13.5%	11.4%	5.6%
2002	22.5%	19.9%	12.1%
2003	28.3%	26.4%	21.7%
2004	24.8%	25.4%	27.9%
2005	27.5%	28.2%	34.7%
2006	32.5%	33.6%	39.8%
2007	38.4%	41.5%	44.6%
2008	47.7%	54.0%	43.9%
2009	52.7%	59.9%	45.4%
Units = all full length albums and digital downloads divided by 10. Revenues include ringtones but exclude performing rights. U.S. Unit Data from RIAA; Revenue data from 2010 IFPI "Recording Industry in Numbers" page 5			

Table 1 also shows that unit declines are slightly less in the U.S. than are revenue declines (columns 1 and 2), indicating a small fall in prices since 1999. The non-U.S. revenues (column 3) decline more slowly in the first few years but then catch up and surpass U.S. losses by 2004, although the U.S. losses become larger again in 2008.

Because of the ease of comparisons across time and geographies, and because Metric 3 directly answers the question as to the importance of file-sharing in the recent industry decline, Metric 3 will be the one I choose as the common denominator with which to compare all results. With this metric chosen as the common denominator, comparisons can be made across the various types of studies to see how similar or dissimilar the results are from one another. First, however, I wish to illustrate how mixing different metrics has led to unfortunate confusion in the literature.

II. Some Inconsistent Uses in the Literature

Regrettably, there are in the literature some inconsistent nomenclatures regarding metrics measuring the impact of file-sharing. For example, Rob and Waldfogel are not the only economists to use the term "displacement rate" when discussing possible metrics for the impact of file-sharing on sales. Oberholzer-Gee and Strumpf (2009), which intends to be a summary of the literature, also uses the term "displacement rate" but its use of the term is different from that of Rob and Waldfogel. Further, Oberholzer-Gee and Strumpf, although they have a specific definition of "displacement rate," do not use it consistently when addressing the literature. Here is portion of a

paragraph from Oberholzer-Gee and Strumpf (2009) that illustrates multiple inconsistent uses of the term that make the comparisons uninformative:

> The majority of studies find that file sharing reduces sales, with estimated *displacement rates* ranging from 3.5% for movies (Rob and Waldfogel, 2007) to rates as high as 30% for music (Zentner, 2006). ...Liebowitz (2008)... reports a *displacement rate* of more than 100% for a selection of U.S. music markets...A typical estimate is a *displacement rate* of about 20%. One implication of these results is that developments other than file sharing must have had a profound impact on sales...Rob and Waldfogel (2006) find an average *displacement effect* of 20%.[8] [My italics]

The first usage of "displacement rate" in the above quote mentions both a 3.5% value from Rob and Waldfogel (2007) and a 30% value from Zentner (2006). The 3.5% figure (for video) used in the Rob and Waldfogel article is an instance of Metric 1, a measure of reduced video sales due to file-sharing (although overall video sales actually increased), whereas Zentner's 30% figure measures the reduced probability of purchasing music and does not fit into any of the three metrics presented above.[9] Although comparing estimated values for movies with estimated values for music might seem a questionable exercise, comparing two completely different metrics to supposedly provide a useful range of estimates is a far more serious error.

Oberholzer-Gee and Strumpf's next usage of the term "displacement rate" concerns Liebowitz (2008) who used Metric 3 in his article, or the share of the decline in music sales due to file-sharing. The third usage of the term found in the quoted paragraph concerns a "typical" estimated displacement rate of 20% that Oberholzer-Gee and Strumpf claim to have derived in some manner. Interestingly, the metric that Oberholzer-Gee and Strumpf claim to be using appears to be Metric 3. For example, in the sentence following this third usage they suggest that a rate of 20% implies that other factors must have had "a profound impact on sales" which is a logical implication only if they are using Metric 3 (among the metrics discussed) because it would imply that 80% of the decline would be due to something other than file-sharing. Further, a few pages

---

[8] See Oberholzer-Gee and Strumpf (2009) page 35. I have included a portion of their footnote 17 in the text of the quoted paragraph placed where the footnote occurred.

[9] In their abstract (page 379), Rob and Waldfogel state "Our analysis indicates that unpaid consumption, which makes up 5.2 per cent of movie viewing in our sample, reduced paid consumption in our sample by 3.5 per cent." Zentner states in his abstract on page 63: "The results suggest that peer-to-peer usage reduces the probability of buying music by 30 percent." He then creates a "back of the envelope" metric equivalent to Metric 1 (having a value of approximately 8%) that he suggests is more informative.

before the above copied quote (page 20), Oberholzer-Gee and Strumpf summarize their results by stating "...many studies conclude that music piracy can perhaps explain as much as one-fifth *of the recent decline in industry sales*" (my italics). Given that in the next sentence they then refer to this decline as a "displacement" and that the amount is identical to the 20% "typical value" found in the paragraph reproduced above, it seems clear that their term "displacement rate" is supposed to measure the extent to which piracy can explain the recent decline in sales, or in other words, Metric 3. At least it would seem clear, except for the fact that they use the term "displacement rate" in so many incompatible ways.

Their final usage of the term "displacement rate" (labeled a displacement "effect") in that paragraph refers to results from the same Rob and Waldfogel (2006) article which I discussed as the leading, and perhaps only, example of Metric 2. Thus Oberholzer-Gee and Strumpf use four different and incompatible metrics as examples of "displacement rate" within this single paragraph. It is not surprising, therefore, that the "typical" 20% figure suggested by Oberholzer-Gee and Strumpf will be seen to bear no relationship to the actual average displacement where displacement is consistently defined as the share of the decline due to file-sharing (Metric 3).

Notice how much this confusion about the metric can affect the message. If file sharing caused a 20% decline in sales (Metric 1), that would likely be a very large share of the sales decline in the years shortly after Napster's introduction. By conflating the metrics used, however, an observed decline of 20 percent of sales might be reported as a "20% displacement" (defined as Metric 3), leaving the reader with the impression that the actual sales reduction due to file-sharing was quite small relative to the overall decline, with other factors playing a much larger roll. Unfortunately, this is exactly the presentation made by Oberholzer-Gee and Strumpf that leaves the reader with the impression that the impact of file-sharing is smaller than it actually was estimated to be.

III. Applying the Metric to the Literature

The point of this section is to compare the results of papers finding that file-sharing caused harm (in the next section I discuss papers that do not find harm). The published papers of which I am aware are Hong (2007, forthcoming), Liebowitz (2006, 2008), Michel (2006), Peitz and Waelbroeck (2004), Rob and Waldfogel (2006), Waldfogel (2010) and Zentner (2005, 2006).

Two unpublished papers of seemingly similar quality to those that are published are Blackburn (2004) and Zentner (2009).

In order to compare the results of these papers to one another, I translate the amount of file-sharing-induced decline that these papers find into a percentage of the decline in sound recording sales that had occurred at the time of their measurement. Naturally, there is going to be some imprecision within many of these original estimates and that imprecision will necessarily carry over to the translated results. For one thing, many of these papers have multiple point estimates. In such cases, I take the one preferred by the authors when their preference seems justified, or, if none is listed as 'preferred' I use the average of the proffered estimates. Even with just a single point estimate, however, these papers use different years and different countries for their analyses and Table 1 makes clear that there are differences in sales declines depending on which years and which countries are used as the basis of analysis. Also, there are confidence intervals around the point estimates, although I ignore those in this analysis.

Table 2 lists alphabetically the results from ten published articles (listed first) and two unpublished studies (listed last) finding some degree of harm due to file-sharing (the details of the calculations underlying Table 2 are found in the Appendix). Seven of these studies have results indicating that the entire decline in sales is due to file-sharing. Another study has two results, with one of those results consistent with the full decline being due to file-sharing and the other result about a third of the decline. Two other studies indicate that file-sharing is responsible for either about half or two thirds of the decline and one study finds the smallest result, between 20% and 40% of the decline.[10] It is clear that the average of these studies is not the 20% "typical estimate" claimed by Oberholzer-Gee and Strumpf since only one of the twelve studies has a result as low as 20%.

---

[10] The reader should be aware that Professor Hong, in his forthcoming article prefers a result of 20% although he found that the overall result after trying to control for compositional changes in his data was 40%. His preference for the 20% value is based in large part on the fact that when he subdivides his population data into cohorts, some of the coefficients are statistically insignificant even though their values still imply an overall 40% decline. He chooses to set these insignificant coefficients to zero, thus lowering the overall impact to 20%. But having less than typical statistical confidence in a result does not imply that a result of zero is more appropriate than the measured coefficient. Thus I list both numbers.

Table 2: Results of Studies Using Metric 3				
Published/Unpublished Studies	Share of Decline due to File-sharing	Original Metric	Final Data Year	Geography
Hong (2007)	>100%	1	2002	U.S.
Hong (forthcoming)	20%-40%	3	2002	U.S.
Liebowitz (2006)	100%	3	2005	U.S.
Liebowitz (2008)	>100%	3	2003	U.S.
Michel (2006)	45%	1	2003	U.S.
Peitz and Waelbroeck (2004)	>100%	1	2002	World
Rob and Waldfogel (2006)	35% or >100%	1	2004	U.S.
Waldfogel (2010)	65%	2	2009	U.S.
Zentner (2006)	>100%	1	2001	7 European
Zentner (2005)	100%	1	2002	World
Blackburn (2004)	>100%	1	2003	U.S.
Zentner (2009)	75%	3	2008	World

In summary, and allocating partial results from studies with mixed results, 7.5 of the 12 studies find that file-sharing explains the entire decline.[11] The average estimated value of Metric 3, for the other 4.5 studies that do not find that the entire decline is due to file-sharing, is 50% of the decline. When the raw numbers from all these studies (found in the Appendix) are averaged, the mean value of Metric 3 is slightly over 100%, further indicating that file-sharing has been estimated to be responsible for more than the entire decline in sales.

The Metric 3 values greater than 100% probably need a word of explanation. Many of the studies have Metric 3 values of greater than 100% and as seen in the Appendix, some values are as high as 200%. A value this large may seem odd at first glance, but such a seemingly high number is not necessarily unreasonable once properly understood. This is best illustrated through the use of a simple example.

---

[11] Professor Hong, in correspondence, suggested that his 2007 result not be given equal consideration to those from his forthcoming paper because he did not try to control for compositional changes in his 2007 paper (although his 2007 paper appears to be written after his forthcoming paper). Because he has not withdrawn or repudiated his 2007 paper, however, and because we cannot know whether he has truly been successful in controlling for compositional changes in his forthcoming paper (he uses propensity scores and not actual variables on individual characteristics), I include the paper in Table 2. Even if his 2007 paper were removed from the Table, however, it would merely lower the share of papers finding that the entire decline was due to file-sharing from 63% (7.5/12) to 59% (6.5/11). Also, the average value of Metric 3 for all papers would still be over 100%.

Example: Assume that a firm sells 10 CDs in year 0, whereupon file-sharing begins. By year 5, sales have dropped to 8 CDs, a 20% decline. Assume as well that in the absence of file-sharing that sales would have increased by 4% per year, leading to counterfactual sales in year 5 of 12.17 units. The apparent decline, the one reported by the record companies and appearing in RIAA-type statistics, is 2 units (10-8). The actual decline, determined from a perfect econometric examination, is 4.17 units (12.17-8). Metric 3 would state that 208% of the measured decline was due to file-sharing (4.17/2). This is close to what Liebowitz (2008) found, where a counterfactual growth rate of 3.6% was sufficient to explain his Metric 3 result of 200%. A sound recording yearly growth rate of 3.6% in the U.S. was a very typical growth rate during the three decades prior to the advent of file-sharing, indicating that a value of 200% for Metric 3 is well within the realm of reasonableness.

The results from a majority of studies—that file-sharing is responsible for the entire decline in sales—is also consistent with the evidence from proposed alternative hypotheses to explain the decline in sound recording sales. Liebowitz (2004) and Liebowitz (2006) carefully examined these alternative explanations and found that they were largely lacking in empirical support, and the intervening years have only strengthened that conclusion.[12] With no support for other possible explanations of the decline in record sales, logical consistency would lead to a conclusion that file-sharing must be responsible for the entire decline, which is what the majority of economic studies have found, once the proper metrics are used.

IV. What about the papers that do not find harm?

There are no published articles in academic journals that find a positive impact of file-sharing on sound recording sales, although there is a study (Andersen

---

[12] For example, the leading alternative explanation (that Liebowitz 2006 did not completely discount) was the purchase of prerecorded video, which did show an increase after 1999 (although it seemed to begin in 1997 and was small compared to the increase in the 1980s when record sales saw robust increases). More recent evidence, however, indicates that sales of prerecorded movies fell after 2004 and were back to their 1999 level by 2009 although sound recording sales showed no such return to their old levels. Similarly, videogame sales, which had been rising since 1996, stopped rising in 2002 whereupon they remained largely unchanged until 2007 at which point there was a sudden and enormous increase, a pattern quite unrelated to the pattern of sound recording sales.

and Frenz, 2007), conducted for a Canadian Ministry, which concludes that file-sharing has a positive impact on sound recording sales.[13]

The two published studies that do not find that file-sharing harms sales are Oberholzer-Gee and Strumpf (2007) and a revised version of the Canadian government study using the original data, Andersen and Frenz (2010). Obviously, when studies find no impact of file-sharing on sound recording sales there is no need to discuss metrics, since all of the metrics will be zero.

This short list of papers with benign results may appear rather puzzling to those who have read the literature review in Oberholzer-Gee and Strumpf (2009), because Oberholzer-Gee and Strumpf provided a considerably longer list of studies with zero or positive impacts of file-sharing. For example, Oberholzer-Gee and Strumpf claim that "[w]hile the majority of papers reports some sales displacement, the four studies using actual measures of file sharing find that file sharing is unrelated to changes in sales" and the Andersen and Frenz study is not even included in this group. The studies that Oberholzer-Gee and Strumpf reference in this quote (in addition to their own 2007 article) are: Bhattacharjee et al., (2007), Tanaka (2004), and Smith and Telang (2008). The reader may ask why I am not including these three studies in the list of studies not finding harm from file-sharing. A few words are in order.

First, I did not include Bhattacharjee et al., (2007) because, contrary to the claims of Professors Oberholzer-Gee and Strumpf, that paper does not conclude that the impact of file-sharing on sales is benign. This is not just a case of my interpretation of the paper differing from their interpretation. Here is what Dr. Bhattacharjee said when a reporter asked him whether Professor's Oberholzer-Gee and Strumpf properly characterized his paper:

> "It is not correct to say that our work shows file sharing is unrelated to changes in sales," said the Management Science paper's lead author, Sudip Bhattacharjee, in an e-mail message to The Chronicle. "The paper did not look directly at sales, only at chart longevity, also known as chart survival." And "we did report a

---

[13] I do not consider the results found in the 2007 report of Andersen and Frenz (2007) to be plausible. This report estimated that each illicitly downloaded song increases sales by slightly less than half a unit (.44). If extrapolated to the economy, this estimate implies that if file-sharing did not exist, there would have been no sales of prerecorded music in Canada at all, a completely unbelievable notion. Further, this estimation was run for only those individuals in the sample who engaged in file-sharing. When the full sample, including both downloaders and non-downloaders was used, the result was that file-sharing hurt record sales by an amount about equal in size (but the opposite sign) to their favored result.

> decrease in survival over all" said Mr. Bhattacharjee... [Glenn 2010].

Second, I chose to exclude Tanaka (2004) from the list not because it is a working paper but because the paper is very clearly not a completed working paper. Tanaka lists the paper as version "0.1". His conclusion begins "This research is very preliminary because we have not yet tried sufficient instrumental variables." Since his main econometric technique is based on instrumental variables and he does not discuss the properties of the instruments that he uses, this appears to be a major problem. Finally, Dr. Tanaka has stated in correspondence that his paper will never be finished nor submitted to a journal whereas the two unpublished papers listed in Table 2 have both been completed and submitted to journals. I invite readers to examine Dr. Tanaka's paper and judge for themselves.

Finally, I leave Smith and Telang (2008) out of the current analysis because that paper attempts to measure the impact of file-sharing on video sales of older movies when they are rebroadcast on television. Because the literature that I examine in this paper is focused on audio, not video, and on the overall impact of file-sharing, not a partial impact on one non-current segment of the market, the Smith and Telang result, interesting though it might be, did not seem relevant.

Therefore, the only one of the four studies listed by Oberholzer-Gee and Strumpf as finding a benign impact of file-sharing on record sales while using actual measures of file-sharing, is Oberholzer-Gee and Strumpf (2007), a paper that I consider to be unreliable in many ways.[14] Oberholzer-Gee and Strumpf list one more paper, Gopal and Bhattacharjee (2006), as finding a positive impact of file-sharing on record sales but I believe they mischaracterize this paper's conclusions.[15] Thus, Oberholzer-Gee and Strumpf (2007) and Andersen

---

[14] See Liebowitz (2007) and Liebowitz (2010) which seriously criticize the analysis and factual claims found in Oberholzer-Gee and Strumpf (2007). In my view Oberholzer-Gee and Strumpf (2009) paper has similar problems (besides those mentioned in the text). For example, they claim that concert revenue increases have more than made up for losses in sound recording sales (as of 2007), although this result is due to their excluding the impact of inflation (real record plus concert revenues fell 33% from 1999 to 2007) along with starting their time period in 1997, three years before file-sharing became important. They also sum the sales of iPods, concerts, and sound recordings, to putatively show a relatively large increase in revenues to the "industry" although iPod revenues do not accrue to the sound recording industry and are, in large part, likely to have replaced the sales of other audio equipment.

[15] Gopal and Bhattacharjee (2006) find that the act of 'sampling,' by itself, has a positive impact on sales but they do not claim that the impact of file-sharing, although it may contain a sampling component, is positive. This judgment is directly supported by their statement "This

and Frenz (2010) are, to my knowledge, the only two published articles that find a benign impact of file-sharing.

If these two papers are included in the sample of studies when calculating average values of Metric 3, it is still the case that a majority of studies finds that the entire decline is due to file-sharing and the average value of Metric 3 is still a very high 89%.[16]

V. Conclusion

Although there have been numerous literature reviews discussing empirical estimates of the impact of file-sharing on sales of sound recordings, none have successfully compared the results on a consistent basis. I have endeavored to fill this lacuna by proposing a simple metric—the share of the sales decline that is explained by file sharing—and translating the empirical results of the literature into that metric. That translation allows a useful comparison of the many efforts to identify the effect of file sharing.

The results indicate that the majority of all studies support a conclusion that the entire decline in sound recording sales can be explained by file-sharing. Even those studies that do not find that file-sharing caused the complete decline usually find that it was responsible for a large share of the decline.

Because this type of comparison has not been previously made, I believe that there has not been a recognition that the literature points to such a strong result. I believe that many interested individuals, many researchers in the area, and even many members of the industry are likely to be surprised that a majority of econometric studies find that the entire decline in sound recording sales that has occurred is due to file-sharing.

[positive sampling result] has major implications for the music industry, in that the industry can potentially reverse the effects of online audio piracy." This quotation makes it clear that Gopal and Bhattacharjee (2006) believe that piracy is likely to have an overall negative impact on the industry that might be overturned if the industry would try to encourage sampling in various venues (although one does have to read the paper fairly carefully to understand some of its conclusions).

[16] This value is calculated using the raw results found in the Appendix.

Appendix: The Creation of Metric 3 for various studies

Below is the version of Table 2 that gives more information about the exact results from calculations of Metric 3. A brief description of the calculations for each paper then follows. I tried to contact each of the authors to make sure I understood and fairly represented their papers. I heard back from all but Peitz and Waelbroeck and Blackburn.

Published/Unpublished Studies	Share of Decline due to File-sharing	Metric Used	Time Frame	Geography
Hong (2007)	110%	1	1997-2002	U.S.
Hong (forthcoming)	20% - 40%	3	1997-2002	U.S.
Liebowitz (2006)	100%	3	2005	U.S.
Liebowitz (2008)	200%	3	1998-2003	U.S.
Michel (2006)	45%	1	2003	U.S.
Peitz and Waelbroeck (2004)	125%	1	1998-2002	World
Rob and Waldfogel (2006)	35% or 140%	1	2003/4	U.S.
Waldfogel (2010)	66%	2	2008/9	U.S.
Zentner (2005)	40%-160%	1	2002	World
Zentner (2006)	190%	1	2001	7 European
Blackburn (2004)	>115%	1	2003	U.S.
Zentner (2009)	58%-92%	3	1997-2008	World

Hong (2007): He looks at the impact of the Internet on several activities, including purchases of sound recordings. Col 2 of his Table 4 directly measures the percentage change in sound recordings due to the Internet, which he finds to be 26%. At that time (2002) U.S. sales units had fallen by 23%, as can be seen in Table 1 above. The leads to the ratio of 26/23.

Hong (forthcoming): This is discussed in footnotes 10 and 11. He adjusts his initial estimates to control for the possibly changing composition of the populations used in his difference-in-difference estimates. When he makes this adjustment he finds an overall decline of 40% due to file-sharing. He then tries to separate these results into subcategories of users/households and although the overall results do not change, the statistical significance for some subsets of the population does change and he sets the results from the insignificant groups to zero, lowering his overall result to 20%. As I explain in the footnotes, I do not believe that setting these values to zero is an appropriate action. He

then, as an additional test, mixes two inconsistent data sets and gets results similar to 20%.

Liebowitz (2006): The approach in this paper was to examine whether alternative hypotheses could explain any of the decline. He concluded that no alternative explanation held up very well with most being completely rejected by the data. New evidence has further confirmed this conclusion. Thus the entire decline is attributed to file-sharing.

Liebowitz (2008): Liebowitz discusses his results in terms of Metric 3 but only to indicate that more than the entire decline is due to file-sharing (or somewhat more precisely, that Internet activities that promote piracy, which may overstate the effect of organized file-sharing narrowly defined). In Table 1 overall album sales fell by .58 units. In Table 5, line 5, file-sharing is claimed to have led to a decline of 1.19 units. This works out to almost exactly 200% as the share of the decline that file-sharing was responsible for. Liebowitz calculated that the growth rate in sales implied by his results, in the counterfactual world without file-sharing, was 3.6%, which seemed reasonable given the historical growth of sales in the prior three decades.

Michel (2006): He uses U.S. data through 2003. He found a decline of 13% that he attributes to file-sharing although the cause is likely to be somewhat broader since he doesn't measure file-sharing per se. Unit sales had fallen by 28% at that time, leading to a value of 45% for Metric 3 (13/28).

Peitz and Waelbroeck (2004): They used data for 16 large markets from 1998 through 2002. They find a 20% decline in unit sales. Assuming that an average of the U.S. and non-U.S. (based on revenues) would mimic somewhat their sample of countries implies a decline in sales of 16%. This leads to a value for Metric 3 of 125% (20/16) although there is some uncertainty in this construction. Still, their estimate is almost certainly over 100% since the U.S. had an early and very high drop in units the first few years after Napster and its decline was just slightly greater than 20%, giving slightly under 100% as the low end estimate of Metric 3.

Rob and Waldfogel (2006): Although the text discusses their results in terms of Metric 2, they also present a result in terms of Metric 1 in which their OLS estimate translates to a 9% decline in sales in the 2003/2004 period (this can be found on their page 53 ("downloading reduced purchases by individuals in the sample by about 9 percent"). The average sales decline in those two years is about 26% so that Metric 3 is 35% (9/26). Their instrumental variable approach provides an estimate that is four times as large, which thus becomes

140%. They conservatively lead with their OLS result but always mention both, so I included both as well. Their results are based on a sample of students that is likely to overstate the impact of file-sharing.

Waldfogel 2010: He uses Metric 2 and finds that the share of each downloaded song that replaces a purchased song averages 27%. From his Table 2, the size of the illicit market is 6.7 relative to the legitimate market's 5.5, giving a ratio of 122%. Multiplying 27% by 122% indicates an overall decline due to file-sharing of 33%. The average 2008/2009 decline in the U.S. was about 50%, giving a Metric 3 value of 66%. His results are based on a sample of students that is likely to overstate the impact of file-sharing.

Zentner (2005): He uses 2002 IFPI world unit sales across countries. The average of the 6 coefficient in his Table 2 is 15.5. In 2002, according to Table 1, the worldwide decline in real revenue was about 16%. This gives a Metric 3 value of about 100%.

Zentner (2006): using 2001 survey data from 7 European countries, found that without file-sharing sales would have been 8% higher, or, in other words, that file-sharing appeared to decrease sound recording sales by roughly 7.4%. European unit sales were down by 3.8%, although there are more European countries than his seven. Nevertheless, the Metric 3 value is 195% (7.4/3.8).

Blackburn (2004): In his Table 7, a 40% reduction in file-sharing leads to a 17% increase in sales and a 50% reduction leads to a 26% increase. Since U.S. units sales had fallen by 23% in 2003 and a 100% decrease in file-sharing would have a larger impact than a 50% decrease, the implication is that Metric 3 would be considerably larger than 115%.

Zentner (2009): Since Zentner uses Metric 3 in his paper one merely needs to read his discussion surrounding his Table 3. The range he presents is 58% to 92%.

References

Andersen Birgitte and Marion Frenz (2010) "Don't blame the P2P file-sharers: The Impact of Free Music Downloads on the Purchase of Music CDs in Canada" *Journal of Evolutionary Economics* Vol. 20, No 5, Pp 715-740.

Andersen Birgitte and Marion Frenz (Released in 2007 although undated) "The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada"

Bhattacharjee Sudip, Gopal Ram D., Lertwachara Kaveepan, and Marsden, James R., (2006) "Impact of Legal Threats on Music Sharing Activity: An Analysis of Music Industry Legal Actions" *Journal of Law and Economics*, 49:1 91-114.

Blackburn, D. (2004) "Online piracy and recorded music sales." Working Paper, Department of Economics, Harvard University.

Connolly Marie and Krueger, Alan B. (2005) "Rockonomics: The Economics of Popular Music" http://cdi.mecon.gov.ar/biblio/doc/nber/w11282.pdf

Dejean, Sylvain (2009) "What Can We Learn from Empirical Studies About Piracy?" *CESifo Economic Studies* 55(2): 326-352.

Gopal Ram D., Sudip Bhattacharjee and G. Lawrence Sanders (2006) "Do Artists Benefit From Online Music Sharing?" *The Journal of Business* Volume: 79, Issue: 3.

Glenn, David (2010). "Dispute over File Sharing's Harm to Music Sales Plays Again" *Chronicle of Higher Education*, July 17.

Hong, S. H. (2007) "The recent growth of the internet and changes in household-level demand for entertainment," *Information Economics and Policy.*

Hong, S. H. (forthcoming) "Measuring the Effect of Napster on Recorded Music Sales: Difference-in-differences Estimates under Compositional Changes" *Journal of Applied Econometrics.*

Liebowitz, Stan J. (2004) "Will MP3 downloads Annihilate the Record Industry? The Evidence so Far" Adv*ances in the Study of Entrepreneurship, Innovation, and Economic Growth*, V. 15, pp. 229-260.

Liebowitz, Stan J (2005). "Pitfalls in Measuring the Impact of File-sharing on the Sound Recording Market." *CESifo Economic Studies* Vol. 51, 2-3, pp. 435-473.

Liebowitz, Stan J. (2006) "File-Sharing: Creative Destruction or just Plain Destruction?" *Journal of Law and Economics* 49 April, 2006, p1-28.

Liebowitz, Stan J. September (2007). How Reliable is the Oberholzer-Gee and Strumpf Paper on File-Sharing? Available at SSRN: http://ssrn.com/abstract=1014399.

Liebowitz, Stan J. (2008). "Testing File-Sharing's Impact on Music Album Sales in Cities" *Management Science*, April (4) Vol. 54, pp. 852-859.

Liebowitz, Stan. J., (2010) "The Key Instrument in the Oberholzer-Gee/Strumpf File-sharing paper is Defective." Available at SSRN: http://ssrn.com/abstract=1598037.

Michel, Norbert J. (2006) "The Impact of Digital File Sharing on the Music Industry: An Empirical Analysis," *Topics in Economic Analysis & Policy*: Vol. 6 : Iss. 1, Article 18. http://www.bepress.com/bejeap/topics/vol6/iss1/art18

Oberholzer-Gee, Felix and Koleman Strumpf (2007). "The Effect of File Sharing on Record Sales: An Empirical Analysis." *Journal of Political Economy* 115(1): 1-42.

Oberholzer-Gee, Felix and Koleman Strumpf (2009). "File-Sharing and Copyright." NBER's Innovation Policy and the Economy series, volume 10, ed. Joshua Lerner and Scott Stern, University of Chicago Press.

Peitz, Martin, and Patrick Waelbroeck (2004). "The Effect of Internet Piracy on Music Sales: Cross-Section Evidence." *Review of Economic Research on Copyright Issues* 1:71–79.

Rob, Rafael, and Joel Waldfogel. (2006). "Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students." *Journal of Law and Economics* 49(1) p 29-62.

Rob, Rafael, and Joel Waldfogel (2007). "Piracy on the Silver Screen" *The Journal of Industrial Economics*, (55) 379-393. September

Tanaka, Tatsou (2004). Does File-sharing Reduce CD sales? A Case of Japan, Working paper. http://www.iir.hit-u.ac.jp/iir-w3/file/WP05-08tanaka.pdf

Zentner, Alejandro (2005). "File Sharing and International Sales of Copyrighted Music: An Empirical Analysis with a Panel of Countries." *Topics in Economic Analysis and Policy* 5, art. 21, pp. 1–15.
http://www.bepress.com/bejeap/topics/vol5/iss1/art21 .

Zentner, Alejandro (2006). ""Measuring the effect of music downloads on music purchases" *Journal of Law and Economics* 49(1): 63–90.

Zentner, A. (2009). "Ten Years of File Sharing and its Effect on International Sales of Copyrighted Music: An Empirical Analysis Using a Panel of Countries" Available at SSRN: http://ssrn.com/abstract=1724444 .

February 4, 2012

The Perpetual War: Pirates and Creators

By EDUARDO PORTER

From book publishers like Macmillan to Hollywood studios like Disney, producers of content are deeply frustrated by the defeat of their efforts to curb online piracy in Congress last month. The bill they favored was flawed, and could have inhibited expression on the Web. But their concern is spot on: the rampant piracy enabled by the Internet undermines the very economics of creative industries.

Online piracy is growing by leaps and bounds, as the first chart shows. The use of peer-to-peer and cyberlocker sites, most of it for illegal sharing, amounts to over one-fourth of all Internet traffic, according to Cisco Systems' Visual Networking Index. And while that fraction is expected to shrink as legal services like Internet video expand, file-sharing is still expected to grow about 23 percent annually, on average, until 2015. The Recording Industry Association of America says that four out of five digital music downloads are illegal.

Piracy's effects on the economy as a whole are hard to measure. Studies used by the supporters of the defeated piracy legislation have tended to exaggerate piracy's economic costs and threat to jobs. For example, they often omit the fact that money not spent on music or movies is likely to be spent on something else. Nonetheless, piracy does hurt the industries that rely on copyright to protect their creations.

Consider the record labels' plunging sales since the music-sharing service Napster made large-scale piracy easy a decade ago. Album sales, including digital singles added up into album equivalents, fell from 755 million in 1999 to 458 million last year, according to Nielsen SoundScan. The top album in 1999, "Millennium" by the Backstreet Boys, sold 9.4 million copies. The top 2011 album, Adele's "21," sold 5.8 million.

Hollywood was hit by piracy somewhat later because movie files are bigger and require more Internet bandwidth. But home entertainment sales — a huge chunk of movie revenues — fell every year from 2004 to 2010. While box-office revenues have benefited from rising ticket prices, movie attendance has been steadily declining. The Oscar-winning "Hurt Locker," for instance, had a worldwide box office of only $49 million but was downloaded

illegally seven million times, according to TorrentFreak, a Web site about file-sharing.

Publishers embraced e-books only a few years ago. In 2010, 1.5 to 3 million people were looking for free pirated copies of books every day, according to an analysis of global Internet searches by Attributor, a Web monitoring company. Of course, not every pirated download displaces the sale of a book, album or movie. But when it comes to music, most economic studies have concluded that piracy accounts for the vast majority or even entirety of the sales decline.

Many Internet enthusiasts say that this change isn't unhealthy, and that the Web makes more ventures possible. They point out that while piracy may be cutting the pay of record label executives, it doesn't seem to have stopped musicians from making new music. According to Nielsen, 75,300 albums were released in 2010, 25 percent more than in 2005. But new releases that sold more than 1,000 copies fell to about 4,700 from 8,000 during that time. The wave of creation that is more hobby than profession has little to do with piracy, and would likely be unaffected by laws to curb illicit downloads.

But if professional musicians, movie directors and writers can't make money from their art, they will probably make less of it. Independent producers say piracy is already making it harder to raise money for small and mid-budget movies.

Stopping piracy is about protecting creativity — and the many occupations it supports (think pop band or sound mixer). If we value what creative industries produce as much as we say we do, Congress will have to find a way to protect it without limiting speech.