Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 23, *Issue* 1 2013 *Article* 1

VOLUME XXIII BOOK 1

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

Annemarie Bridy*

*University of Idaho College of Law, abridy@uidaho.edu

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

Annemarie Bridy

Abstract

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 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. Subsequently, the Obama administration, represented nationally by the Office of the Intellectual Property Enforcement Coordinator (IPEC) and internationally by the Office of the United States Trade Representative (USTR), expressly endorsed the concept of privately negotiated anti-piracy collaborations between corporate rights owners and broadband providers. In July of 2011, broadband providers finally bowed to the mounting political pressure and to changing economic realities in the business of corporate content ownership and delivery. 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. The MOU creates what the parties characterize as a common framework of 'best practices' to effectively alert subscribers, protect copyrighted content and promote access to legal online content. This Article is an assessment of the MOU's Copyright Alert System (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 overview of CAS, including the structure by which it is governed, the division of labor it prescribes between copyright owners and broadband providers, the

---

*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" Memorandum of Understanding (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.

progression of warnings and sanctions it implements, and the appeals process it makes available for affected broadband subscribers. 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.

KEYWORDS: online piracy, Hadopi, graduated response, copyright infringement, Eircom, three strikes, six strikes, file sharing, P2P, peer to peer, Copyright Alert System, copryight enforcement

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

Annemarie Bridy*

* 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" Memorandum of Understanding (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.

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,

[1] *See* H.R. REP. NO. 105-796, at 72 (1998) ("Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright

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*

infringements that take place in the digital networked environment."); S. REP. NO. 105-190, at 20 (1998) (same).

2 *See* 17 U.S.C. § 512(c) (2006) (setting forth the DMCA's notice-and-takedown framework); 17 U.S.C. § 512(m) (2006) (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) (2006) (setting forth a framework for copyright owners to obtain pre-litigation subpoenas to identify alleged infringers); 17 U.S.C. § 512(i) (2006) (requiring ISPs to adopt and reasonably implement a program for terminating the access or accounts of repeat infringers).

3 *See* Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 695 (2011) (describing this problem at length as the DMCA's failure to scale for P2P infringements); *see also* Jerome H. Reichman et al., *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKLEY 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 *See* 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.").

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] 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

---

[5] 532 F. Supp. 2d 556 (S.D.N.Y. 2007). In the case, Arista Records and a dozen music industry co-plaintiffs sued the operators of the LimeWire P2P service for secondary copyright infringement. The service would later be shut down by court order following a grant of summary judgment to the plaintiffs. *See* Arista Records v. Lime Group, 715 F. Supp. 481, 492–93 (S.D.N.Y. 2010).

[6] *See* Bernadette Tansey, *New Tactic Fights File Sharing*, S.F. CHRON., Dec. 20, 2008, at C1 ("The [Recording Industry Association of America (RIAA)] said New York Attorney General Andrew Cuomo is helping the industry develop an alternative to its mass courtroom campaign by promoting its talks with Internet providers.").

[7] *See* OFFICE OF THE INTELLECTUAL PROP. 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"); OFFICE OF THE INTELLECTUAL PROP. ENFORCEMENT COORDINATOR, 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 of 2011, art. 27, at E14–17, *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.

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 and to changing economic realities in the business of corporate content ownership and delivery.[10] 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.[11] The MOU creates what the parties characterize as "a common framework of 'best practices' to effectively alert subscribers, protect copyrighted content and promote access to legal online content."[12] At the core of the common framework is the Copyright

---

[9] OECD, OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY MAKING 4, 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] 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 fifteen years since the DMCA became law. *See* Annemarie Bridy, *ACTA and the Specter of Graduated Response*, 26 AM. U. INT'L L. REV. 558, 571–72(2011) [hereinafter Bridy, *ACTA*] (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." *See* Kenneth Corbin, *Comcast Set to Enter Copyright Wars*, DATAMATION.COM (Jan. 27, 2010), http://www.datamation.com/cnews/article.php/3861096/Comcast-Set-to-Enter-Copyright-Wars.htm (quoting Roberts).

[11] The participating ISPs are AT&T, Verizon, Comcast, CSC Holdings (Cablevision), and Time Warner. *See* MEMORANDUM OF UNDERSTANDING 24 (Attachment A) (July 6, 2011) [hereinafter MOU], *available at* http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf. 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 Recording Industry Association of America (RIAA) (UMG, Warner, Sony, and EMI). *See 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. *See id.* at 2.

[12] *See* Press Release, Ctr. for Copyright Info., Music, Movie, TV and Broadband Leaders Team to Curb Online Content Theft Announce Common Framework for "Copyright Alerts" (July 7, 2011), *available at* http://infojustice.org/archives/4145.

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.[13] 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.[14] It applies only to users of residential broadband services and is intended to address infringement only over P2P networks.[15]

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 graduated system of warnings and sanctions it employs, and the appeal process it makes available to accused infringers. 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]

---

[13] *See* MOU, *supra* note 11, at 1 (introducing the idea of "[a] reasonable alert-based approach"); *see also id.* at 7–14 (setting forth the technical requirements of CAS). The French system will be discussed in Part II.A *infra*.

[14] *See* MOU, *supra* note 11, at 7 (requiring party ISPs to amend their terms of service or acceptable use policies to incorporate CAS).

[15] *See id.* at 2 (defining the scope of the program).

[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 is 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), http://arstechnica.com/tech-policy/2011/07/what-the-1930s-fashion-industry-means-for-big-contents-six-strikes-plan.

I. THE GRADUATED RESPONSE PARADIGM

This Part begins with a general discussion of graduated response 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.

A. Graduated Response Generally

Graduated response is designed to address the phenomenon of repeat infringement over digital networks. In general, graduated response involves a series of 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

---

[17] *See* IFPI, DIGITAL MUSIC REPORT 2011: MUSIC AT THE TOUCH OF A BUTTON 18 (2011) (defining graduated response).

[18] *See generally* Peter Yu, *The Graduated Response*, 62 FLA. L. REV. 1373 (2010) (describing the "three strikes" model).

[19] *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81, 84 (2010) [hereinafter Bridy, *Graduated Response*]. 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).

infringers.[20] Unlike the notice and takedown provision in the DMCA, which applies to service providers that store data for users but not to those that simply route and transmit their users' data, the repeat infringer provision applies equally to all ISPs, including broadband providers.[21]

Given the high volume of illegal file sharing online, one might expect broadband providers' compliance with the repeat infringer provision to result fairly routinely in account terminations for P2P users. In practice, however, that has not been the case. Establishing 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 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 absent a court order identifying the subscriber as a repeat infringer.[23] The upshot is that there is no

---

[20] *See* 17 U.S.C. § 512(i)(1)(A) (2006); 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) (2006). Section 512(a) providers are not subject to the notice and takedown framework outlined in section 512(c). *See 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 the safe harbor in section 512(c) and are subject to the notice and takedown framework set forth in that section. *See* 17 U.S.C. § 512(c) (2006). All providers seeking safe harbor under the DMCA are subject to section 512(i), which is the repeat infringer provision. *See* Perfect 10 v. CCBill, 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)").

[22] *See* Bridy, *Graduated Response*, *supra* note 19, 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. *See* 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-its-complicated. AT&T has said

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. ISPs have thus 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—filtering and protocol-based throttling, for example—to control network congestion caused in part by P2P file sharing.[26] With the increasing popularity of legal

---

that it will not terminate a customer's service for repeat infringement without a court order. *See* Greg Sandoval, *How Charter Communications Warns Accused File Sharers*, CNET (Apr. 19, 2009), http://news.cnet.com/8301-1023_3-10222853-93.html.

[24] *See* Bridy, *Graduated Response, supra* note 19, at 100–03 (explaining the relationship between graduated response and DMCA compliance).

[25] *See* Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J. (Dec. 19, 2008), http://online.wsj.com/article/SB122966038836021137.html (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), http://arstechnica.com/uncategorized/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman (interviewing the RIAA's Cary Sherman about graduated response).

[26] *See e.g.*, *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. 1 (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/

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 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. An official

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*, *supra* note 19, at 105.

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 11, 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." *Id.* at 7.

29 *See* Anderson, *supra* note 25 (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. *See* IFPI, *supra* note 17, at 21.

30 *See* Chloe Albanesius, *Comcast, Others Deny "Three Strikes" Piracy Plan*, PCMAG.COM (Mar. 27, 2009, 11:54 AM), http://www.pcmag.com/article2/0,2817,2343977,00.asp; David Kravets, *Top Internet Providers Cool to RIAA 3-Strikes Plan*, WIRED (Jan. 5, 2009, 11:43 AM), http://www.wired.com/threatlevel/2009/01/draft-verizon-o.

31 *See* Ctr. for Copyright Info., *supra* note 12.

declaration released during the 2005 Cannes Film Festival by the European Union's (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."[32] 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.[33] 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.[34] For his outspoken public support of graduated response legislation and, even more controversially, in-network filtering, Sarkozy earned public praise from the International Federation of the Phonographic Industry (IFPI).[35]

In 2006, a report on intellectual property policy commissioned by the government of the United Kingdom (UK) recommended that ISPs voluntarily adopt a "Best Common Practice (BCP) document" for coordinating with rights owners "to remove and disbar users engaged in 'piracy.'"[36] The report also recommended that legislation mandating user disconnection be introduced if a voluntary agreement could not be achieved by the end of 2007.[37] As events actually played out, the British government pressed for

---

[32] *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* (May 17, 2005), http://ec.europa.eu/avpolicy/docs/other_actions/cannes_decl_2005_en.pdf.

[33] *See id.*; *see also* MONICA HORTEN, THE COPYRIGHT ENFORCEMENT ENIGMA: INTERNET POLITICS AND THE "TELECOMS PACKAGE" 84 (2012).

[34] *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.

[35] *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.

[36] HM TREASURY, THE GOWERS REVIEW OF INTELLECTUAL PROPERTY 103 (2006).

[37] *See id*.

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.[38] That MOU expired in 2009, however, after a three-month trial period.[39] 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.[40] 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.[41] 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.[42] 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

---

[38] *See* Andrew Orlowski, *Feargal Sharkey on the ISP Filesharer MoU*, THE REGISTER (July 24, 2008, 10:16 AM), http://www.theregister.co.uk/2008/07/24/feargal_music_isp_mou (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).

[39] *See* CHRISTOPHER T. MARSDEN, INTERNET CO-REGULATION 210 (2011).

[40] *See id.* at 211–14 (describing events leading to the passage of the DEA); Digital Economy Act, 2010, c. 24 (U.K.).

[41] *See* Digital Economy Act, 2010, c. 24, §§ 5–6 (U.K.); Digital Economy Act, 2010, c. 24, Explanatory Notes, ¶ 32 (U.K.) ("The obligations will be underpinned by a code approved by OFCOM or, if no industry code is approved, made by OFCOM. The code will set out in detail how the obligations must be met.").

[42] *See* Digital Economy Act, 2010, c. 24, §§ 3–18 (setting forth "initial obligations" that include subscriber notification and authorizing the Secretary of State to impose additional "technical obligations" on ISPs); Digital Economy Act, 2010, c. 24, Explanatory Notes, ¶ 33 ("In case the initial obligations prove insufficient to reduce significantly the level of online infringement of copyright, the provisions also grant the Secretary of State a power to impose further obligations ("technical obligations") on ISPs. . . . Technical measures could only be used against subscribers who met the threshold for inclusion in a copyright infringement list under the initial obligations. Technical measures would be likely to include bandwidth capping or shaping that would make it difficult for subscribers to continue file-sharing, but other measures may also be considered. If appropriate, temporary suspension of broadband connections could be considered.").

in file sharing volumes are not timely achieved.[43] The English have thus taken a graduated approach to graduated response.[44]

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.[45] At the outset, the copyright industries viewed the telecoms framework review process as an opportunity to push for a Europe-wide, top-down graduated response mandate.[46] The simple version of the highly fraught political narrative that unfolded 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.[47] In the end, individual member states were left to decide whether to require ISPs to implement graduated response.[48] 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

---

[43] *See* MARSDEN, *supra* note 39, at 54 (defining co-regulation as a middle ground between direct government regulation of industry and industry self-regulation); *see also* Digital Economy Act, 2010, c. 24, Explanatory Notes, ¶ 31 ("The Act includes provisions concerned with online infringement of copyright. This is particularly, but not exclusively, in response to infringement of copyright in the fields of music, film and games. The Act inserts new sections . . . which, once a supporting code approved or made by OFCOM has been put in place, impose obligations on internet service providers ("ISPs") who meet the criteria set out in the code.").

[44] *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).

[45] *See* HORTEN, *supra* note 33, at 64–69 (2012) (offering 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 infringement).

[46] *See id.* at 103.

[47] *See id.* at 122–25, 191–95.

[48] *See* HORTEN, *supra* note 33, at 213–14. The amendment that was ultimately adopted "neither mandates nor prohibits" national graduated response regimes. Directive 2009/136, art. 1, 2009 O.J. (L 337) 11, 21 (EC).

to the interests of copyright owners in member states that do elect to implement mandatory graduated response regimes.[49]

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).[50] In addition to dispatching its representatives to testify before national legislatures considering adopting graduated response mandates,[51] the IIPA participates annually in the USTR'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.[52] 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.[53] Since 2009, the IIPA has used the Special 301 process to focus its members' disapproval on individual governments, including among others those of Sweden, Japan, Hong Kong, and Singapore.[54]

---

[49] *See* Directive 2009/136, art. 1, 2009 O.J. (L 337) 11, 21 (EC) ("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.").

[50] 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). *See Description of the IIPA*, IIPA, http://www.iipa.com/aboutiipa.html (last visited Nov. 15, 2012).

[51] New Zealand is a case in point. *See generally* SUBMISSION OF THE INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE ON THE COPYRIGHT (INFRINGING FILE SHARING) AMENDMENT BILL BEFORE THE HOUSE OF REPRESENTATIVES SELECT COMMITTEE ON COMMERCE, June 16, 2010, *available at* http://www.iipa.com/pdf/NewZealandIIPA SubmissionOnFileSharing061610.PDF.

[52] *See generally Special 301*, IIPA, http://www.iipa.com/special301.html (last visited Nov. 15, 2012) (linking to transcripts of recent legislative testimony and to press releases outlining IIPA's recommended sanctions).

[53] *See generally id.*

[54] *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.[55] 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.[56] 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]."[57] Such language implies graduated response to anyone familiar with the rhetoric crafted to sell the concept to policy makers.[58]

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.[59] A leaked draft of the TPP contains a repeat infringer provision virtually identical to the one in the DMCA.[60] The same

---

[55] *See* Bridy, *ACTA*, *supra* note 10, at 561 ("The official draft text of ACTA, released on April 21, 2010 ("the April draft"), confirmed that mandatory graduated response was no longer on the table for the negotiating parties by the end of the eighth round. What remained, however, was a more general provision that conditioned ISP eligibility for safe harbor from claims of third party infringement on 'an online service provider adopting and reasonably implementing a policy . . . to address unauthorized storage or transmission of materials protected by copyright.' Such a policy presumably might, though it needn't necessarily, entail graduated response.").

[56] *See id.* at 561 (observing that the Office of the United States Trade Representative announced publicly in a press release that "no participant is proposing to require governments to mandate a 'graduated response' or 'three strikes' approach to copyright infringement on the Internet").

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

[58] *See id.* at 570 (asserting that "cooperation" has become something of a code word for graduated response).

[59] *The United States in the Trans-Pacific Partnership*, OFFICE OF THE U.S. TRADE REPRESENTATIVE, http://www.ustr.gov/about-us/press-office/fact-sheets/2011/november/united-states-trans-pacific-partnership (last visited Nov. 16, 2012). The parties to the TPP are Australia, Brunei Darussalam, Chile, Malaysia, New Zealand, Peru, Singapore, Vietnam, and the United States. *See id.*

[60] *Compare Trans-Pacific Partnership Intellectual Property Rights Chapter Draft—February 10, 2011* , 34, http://keionline.org/sites/default/files/tpp-10feb2011-us-text-ipr-chapter.pdf (last visited Nov. 16, 2012) ("Eligibility for limitations . . . shall be

provision appeared in early drafts of ACTA.[61] 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 is difficult to predict 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.[62] 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.[63] 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 alleged infringers to rights

conditioned on the service provider . . . adopting and reasonably implementing a policy that provides for termination in appropriate circumstances of the accounts of repeat infringers."), *with* 17 U.S.C. § 512(i)(1)(A) (2006) ("The limitations on liability . . . shall apply . . . only if the service provider . . . has adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers.").

61 *See* Bridy, *ACTA*, *supra* note 10, at 562–63.

62 *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).

63 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, ¶ 49, U.N. Doc. A/HRC/17/27 (May 16, 2011).

owners are "highly invasive" of individuals' privacy and should be abandoned in favor of less intrusive, more proportional measures.[64]

II. IN THE EU: TWO TAKES ON "THREE STRIKES"

This Part considers "three strikes" implementations of graduated response in two European Union (EU) countries: France and Ireland. The French system, Hadopi, has been operational since 2010.[65] 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.[66] 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.[67] 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 perspectives of privacy and expressive rights.

---

[64] *See 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 [hereinafter *Opinion of the European Data Protection Supervisor*].

[65] *See 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).

[66] *See* Press Release, Eircom, Statement on Illegal File Sharing, http://pressroom.eircom.net/press_releases/article/eircom_Statement_on_Illegal_File_Sharing.

[67] *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).

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.[68] 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.[69] 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.[70] 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 repeat infringers.[71] The report was followed in 2008 by the introduction of legislation creating that administrative body, Hadopi.[72] Under the original version of the legislation, Hadopi 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.[73] 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.[74] After passage of the bill in 2009, opponents challenged its constitutionality, and the French Constitutional Council ruled that a user's Internet access

---

68 *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).

69 *See id.*

70 *See id.* at 300.

71 *See id.*

72 *See id.*

73 *See id.* at 301.

74 *See Les Députés Adoptent la Loi Hadopi*, LE MONDE.FR (May 12, 2009, 9:10 PM), 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, 12:43 PM), http://news.cnet.com/8301-1023_3-10238912-93.html.

could not be suspended solely on the authority of an administrative body without a court order.[75] 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.[76] Under the amended law, the judge has authority 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.[77]

An Internet security and content detection company selected by rights owners generates the notices of infringement in the Hadopi system.[78] 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.[79] The notice is forwarded from the security company to the copyright owner, which then refers the incident to Hadopi.[80] To protect the accused subscriber's privacy, Hadopi forwards the notice to the subscriber without disclosing his or her identity to the copyright owner.[81] If a subscriber is alleged

---

[75] *See* Conseil constitutionnel [CC] [Constitutional Court] decision No. 2009-590DC, Oct. 22, 2009, Rec. 179 (Fr.). 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, 662–64 (2011) (discussing in detail the Council's decision and the underlying principles of French law).

[76] *See* Loi 2ac009-1311 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 [C.P.I.] art. L331–21 (Fr.).

[77] *See* Rayna & Barbier, *supra* note 68, at 301.

[78] *See id.*

[79] *See id.*; *see also Quelles informations me concernant sont détenues par l'Hadopi si je fais l'objet d'une procédure de réponse graduée?,* HADOPI, http://www.hadopi.fr/quelles-informations-me-concernant-sont-detenues-par-lhadopi-si-je-fais-lobjet-dune-procedure-de-rep (last visited Nov. 16, 2012) (explaining what information concerning an alleged infringement is transmitted to Hadopi by the copyright owner).

[80] *See* Rayna & Barbier, *supra* note 68, at 301; *see also Réponse Graduée*, HADOPI, http://www.hadopi.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/reponse-graduee.html (last visited Nov. 16, 2012).

[81] *See* Rayna & Barbier, *supra* note 68, at 301.

to have infringed on a second occasion within six months of receiving the first notice, Hadopi forwards a second notice.[82] 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 to be suspended.[83] 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.[84] If the judge determines that the infringement was not merely negligent, a one year suspension may be imposed.[85] 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.[86]

Hadopi began sending notices to alleged infringers in October 2010 at a reported rate of 25,000 per day.[87] As of December 1, 2011, over 750,000 first notices had been sent.[88] 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.[89] As of September 2012, fourteen cases had been referred for prosecution,

---

[82] *See id.* (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE [C.P.I.] art. L331–25 (Fr.)); *see also Comment fonctionne la réponse graduée?*, HADOPI, http://www.hadopi.fr/comment-fonctionne-la-reponse-graduee-0 (last visited Nov. 16, 2012) (explaining the protocol).

[83] *See* Rayna & Barbier, *supra* note 68, at 301 (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE [C.P.I.] art L335-7 (Fr.)); *see also Comment fonctionne la réponse graduée?*, *supra* note 82.

[84] 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 68, at 301 (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE [C.P.I.] art. L335-7-1 (Fr.)); *Qu'est-ce que l'infraction de négligence caractérisée?*, HADOPI, http://www.hadopi.fr/quest-ce-que-linfraction-de-negligence-caracterisee (last visited Nov. 16, 2012).

[85] *See* Rayna & Barbier, *supra* note 68, at 301. During this period, the subscriber remains responsible for the regular price of the subscription and may not subscribe to another service. *See id.* at 301 n.13.

[86] *See id.* at 301–02.

[87] Aymeric Pichevin, *French Anti-Piracy Scheme's 25,000 Daily Reports*, BILLBOARD.BIZ (Oct. 22, 2010), http://www.billboard.biz/bbbiz/content_display/industry/news/e3i1c1499752deb3a60a1584400533395b0.

[88] *See* HADOPI, HADOPI: 1 1/2 YEAR AFTER THE LAUNCH 3 (2012), *available at* http://www.hadopi.fr/sites/default/files/page/pdf/note17_en.pdf.

[89] *See id.*

and the court had imposed a single fine amounting to a little under $200.[90] Of more than 1,000 French Internet users between the ages of fifteen and fifty 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.[91] 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%.[92] 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.[93] When increased illegal streaming and direct download traffic are taken 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.[94] 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.[95] When these alternative explanations are

---

[90] *See* Peter Sayer, *French Court Levies First Fine Under Three-Strikes Law on Illegal Downloads*, PCWORLD (Sept. 13, 2012, 10:00 AM), https://www.pcworld.com/article/262285/french_court_levies_first_fine_under_threestrikes_law_on_illegal_downloads.html.

[91] *See* HADOPI, *supra* note 88, at 6.

[92] *See id.* at 5.

[93] *See* Benjamin Ferran, *Le Bilan Contrasté de l'Action de l'Hadopi*, LE FIGARO (Mar. 28, 2012, 7:15 PM), http://www.lefigaro.fr/hightech/2012/03/27/01007-20120327ARTFIG00670-le-bilan-contrastee-de-l-action-de-l-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).

[94] *See id;* Monica Horten, *Hadopi—Has it Massaged the Numbers?,* IPTEGRITY.COM BLOG (Mar. 31, 2012), http://www.iptegrity.com/index.php/france/755-hadopi-has-it-massaged-the-numbers.

[95] *See* Horten, *supra* note 94 (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*, N.Y. TIMES (Feb. 19, 2012),

considered, the argument that Hadopi has dramatically decreased the volume of online infringement loses some of its force.

Another way to assess the impact of Hadopi on French consumer behavior is to try to measure the law's effect on legal music sales. The American economist Brett Danaher and his co-authors took this approach, concluding in a report trumpeted by the IFPI that public awareness of Hadopi drove French consumers to legal (iTunes) downloads.[96] 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.[97] Time will tell 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. 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.[98] Danaher and his co-authors assert that Hadopi will be more effective than lawsuits at achieving

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).

96 *See* BRETT DANAHER ET AL., THE EFFECT OF GRADUATED RESPONSE ANTI-PIRACY LAWS ON MUSIC SALES: EVIDENCE FROM AN EVENT STUDY IN FRANCE 2 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240. 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 14 n.16. Journalists for the French newspaper *Le Monde* have critiqued the study, suggesting some alternative explanations for the observed increase in iTunes sales, including the launch of new iPhone models and the holiday season. *See* Damien Leloup and Jérémie Baruch, *Hadopi, Source de la Croissance d'iTunes?*, LE MONDE.FR Jan. 24, 2012, 7:39 PM), http://www.lemonde.fr/technologies/article/2012/01/24/hadopi-source-de-la-croissance-d-itunes_1633919_651865.html.

97 *See* DANAHER ET AL., *supra* note 96, at 2.

98 *See* 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).

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.[99] It is possible, too, that Hadopi will be somehow restructured 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.[100]

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.[101] 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 end an ongoing legal dispute.[102] After an eight day trial, Eircom and IRMA agreed in 2009 to a settlement that required Eircom to implement a "three strikes" protocol.[103] The case never went to judgment on the merits, so there is no copyright law on the books as a result of it,[104] yet the settlement has the reach and effect of public law: every one of Eircom's 2.6 million subscribers is now bound through

---

[99] *See* DANAHER ET AL., *supra* note 96, at 4, 8, 20–21.

[100] *See* 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).

[101] *See* EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 1 (H. Ct.) (Ir.); *Ireland Cracks Down on Internet Piracy*, INDEPENDENT (May 29, 2010), http://www.independent.co.uk/news/media/ireland-cracks-down-on-internet-piracy-1986733.html [hereinafter *Ireland Cracks Down*].

[102] *See EMI Records*, [2010] IEHC 108, at ¶ 1.

[103] *See id.* at ¶¶ 2, 9.

[104] In a subsequent case, IRMA sought a court order requiring UPC, another Irish ISP, to implement a graduated response system like Eircom's. *See* 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 authorised or ruled on by the Court." *Id.* at ¶ 135.

Eircom's Terms of Service to the terms of the Eircom-IRMA settlement.[105]

The Eircom protocol was implemented on a preliminary basis beginning in June 2010 and on a permanent basis the following October.[106] 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 file sharing.[107] This first warning is included with the subscriber's monthly bill.[108] 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.[109] 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.[110] Upon receipt of a third notice concerning the same subscriber, Eircom reviews the evidence against the subscriber.[111] 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 subscriber's Internet service is cut off for seven days.[115] If the user continues to

---

105 *See* John Collins, *Three Strikes Rule Aims to Knock Out Music Sharing*, IRISH TIMES, June 4, 2010, at 6.

106 *See* Eircom, *supra* note 66; IFPI, *supra* note 17, at 18.

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

108 *See id.* at ¶ 13.

109 *See id.* at ¶¶ 9, 13.

110 *See id.* at ¶ 13.

111 *See id.*

112 *See id.*

113 *See id.*

114 *See id.*

115 *See* Eircom, *supra* note 66 (setting forth sanctions under the protocol).

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 twelve 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 ensuring judicial review of disconnection decisions, Eircom's subscribers have no such guarantee.[120] 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.[121] By signing up for broadband service, Eircom's

---

116 *See id.*

117 *See EMI Records*, [2010] IEHC 108, 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 *See* Mark Tighe, *Eircom Cut Off 100 Illegal Downloaders*, SUN. TIMES (Eng.), Mar. 4, 2012, at 5.

119 *See id.*

120 *See id.*

121 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).

subscribers consent to graduated response and surrender any conflicting public law guarantees.[122]

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.[123] 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.[124] 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 Eircom characterized as a "minor technical issue."[125] 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.[126] The notice concluded with an

---

122 *See EMI Records*, [2010] IEHC 108, 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.").

123 *See id.* at ¶¶ 18, 25.

124 *See id.* at ¶ 27.

125 *See* Mary Carolan, *Four Music Firms Dispute Data Chief's Notice to Eircom*, IRISH TIMES, Mar. 1, 2012, at 4; *see also* EMI Records v. Data Protection Commissioner, [2012] IEHC 264, ¶¶ 1.0, 1.3 (explaining that Eircom changed the clocks in its network to reflect daylight savings time two months late, thereby causing a mismatch between dynamically assigned IP addresses and subscriber accounts, which led to the delivery of erroneous notices of infringement).

126 Data Protection Comm'rs 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).

order for Eircom to stop administering the protocol.[127] IRMA's member companies promptly appealed, arguing that the order represented an attempt to re-litigate the data protection issues already decided by the High Court in 2010.[128] 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.[129] To the extent that a rationale could be discerned in the notice, the court held, it rested on a misconstruction of the applicable law.[130] 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 the untenable holding that copyright may not be enforced on the Internet.[131]

III. IN THE U.S.: 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 complementary 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

---

127 *See* Mark Tighe, *Piracy Action Lands Eircom in Hot Water*, SUN. TIMES (Eng.), Dec. 18, 2011, at 7.

128 *See* Carolan, *supra* note 125, at 4.

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

130 *See id.*

131 *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.").

primarily with educating a general audience about copyright law, the problem of online infringement, and legal sources of online content.[132] 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.[133] As the center of gravity for the inter-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.[134]

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.[135] Funding for CCI is split fifty-fifty, and the organization is governed by a six-member executive committee of which each group chooses three members.[136] 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."[137] Under the terms of the MOU, each group appoints one member of the advisory board, and those two members together choose the third member.[138] 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.[139] As Mary LaFrance has observed, the MOU provides no real guarantee that the advisory board will have any direct impact on CCI's activities.[140]

Members of CCI's inaugural advisory board, which actually has four members instead of the anticipated three, include Jerry

---

132 *See* MOU, *supra* note 11, at 4.
133 *See id.*
134 *See id.* at 5.
135 *See id*.
136 *See id.* at 3–4.
137 *Id.*
138 *See id.* at 3.
139 *See id*. at 4.
140 *See* Mary LaFrance, *Graduated Response by Industry Compact: Piercing the Black Box*, 30 CARDOZO ARTS & ENT. L.J. 165, 171 (2012).

Berman of the Center for Democracy and Technology and Gigi Sohn of Public Knowledge.[141] The other two members are Marsali Hancock, the president of the iKeepSafe Coalition, which monitors digital technologies and their effect on children,[142] and Jules Polenetsky of the Future of Privacy Forum.[143] 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.[144] 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.[145] According to the MOU, the retention of experts is intended to ensure and maintain the parties' and the public's confidence in the accuracy and security of those methods.[146] Like the recommendations of the advisory board, however, any recommendations these experts make are confidential and non-binding.[147] The incentive created in the MOU for copyright

---

[141] *See* Press Release, Ctr. for Copyright Info., Center for Copyright Information Announces Three Major Steps Towards Implementation (Apr. 2, 2012), http://www.copyrightinformation.org/node/705 [hereinafter Three Major Steps Press Release].

[142] *See id*.

[143] *See id.*

[144] *See, e.g.*, *Digital Copyright*, CDT, https://www.cdt.org/issue/digital-copyright (last visited Nov. 16, 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"); *Key Issues: Balanced Copyright*, PUBLIC KNOWLEDGE, http://www.publicknowledge.org/issues/balanced-copyright (last visited Nov. 16, 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.").

[145] *See* MOU, *supra* note 11, at 4–5.

[146] *See id.* at 5.

[147] *See id.* ("Failure to adopt a recommendation of the Independent Expert shall not amount to a breach under this Agreement. The Independent Expert's recommendations

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.[148] As of this writing CCI has not publicly identified its privacy experts. Its "independent" technical expert is the firm Stroz Friedberg, a former lobbyist for the RIAA.[149] The choice of Stroz Friedberg drew immediate fire from critics who rightfully questioned the firm's ability to be truly independent in light of its past paid advocacy for corporate rights owners.[150] Responding promptly and directly to this criticism, CCI announced that it would hire an additional—and presumably more independent—independent technical expert.[151] As this Article goes to press, the additional technical expert has not yet been named.

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.[152] 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

must be shared with each of the Content Owner Representatives and the affected Participating ISP, but may not be disclosed to other parties.").

148 *See* MOU, *supra* note 11, at 5–6. Whether that is a strong enough incentive will be addressed in Part IV, *infra*.

149 *See The Copyright Alert System: Moving To Implementation*, Ctr. for Copyright Information, Oct. 18, 2012, http://www.copyrightinformation.org/node/709 (announcing the selection of Stroz Friedberg as the independent technical expert); *Six-Strikes "Independent Expert" Is RIAA's Former Lobbying Firm*, TORRENTFREAK (Oct. 22, 2012), https://torrentfreak.com/six-strikes-independent-expert-is-riaas-former-lobbying-firm-121022 (reporting on Stroz Friedberg's prior business relationship with the RIAA).

150 *See id.* (criticizing the choice of Stroz Friedberg). TorrentFreak reported that the RIAA did not disclose its prior relationship with Stroz Friedberg to its CCI partners. *See RIAA Failed To Disclose Expert's Lobbying History to "Six-Strikes" Partners*, TORRENTFREAK (Oct. 27, 2012), https://torrentfreak.com/riaa-failed-to-disclose-experts-lobbying-history-to-six-strikes-partners-121026.

151 *See* Jill Lesser, *CCI Recommits to Independent Evaluation of Content Methodology*, Ctr. for Copyright Info., Oct. 30, 2012, http://www.copyrightinformation.org/node/712 (acknowledging the link between the RIAA and Stroz Friedberg and affirming CCI's commitment to a genuinely independent assessment of the technology underlying CAS).

152 *See* MOU, *supra* note 11, at 3.

suspected individual infringements over P2P networks. 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.[153] 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.[154] Each ISP is also required to modify its terms of service for residential broadband to incorporate the notice-and-sanction structure of CAS.[155] 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.[156] 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.[157] 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.[158] In addition to that limit, ISPs have discretion to temporarily stop processing notices if the demand on their systems and resources becomes unreasonable.[159] Any temporary stoppage must be followed, however, by prompt notice to copyright owners and a collaborative effort to correct the "over-provisioning."[160]

---

153 *See id.* at 4–5.

154 *See id.* at 7.

155 *See id.*

156 *See* MOU, *supra* note 11, 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.

157 *See id.* at 7.

158 *See id.* at 16.

159 *See id.*

160 *Id.*

The first two copyright alerts are educational in nature and require no response or action from the subscriber.[161] 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.[162] The third and fourth alerts contain sterner language and require the subscriber to acknowledge receipt.[163] 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.[164] 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.[165]

Sanctions, or "mitigation measures," are not triggered until a fifth alert is sent.[166] The MOU avoids being prescriptive when it comes to sanctions, specifying instead a range of mitigation measures from which ISPs can choose.[167] 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.[168] No ISP operating under the MOU is required to suspend access for any subscriber.[169] (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.[170] The sixth alert, however,

---

161 *See id.* at 8–9. An ISP may reduce the number of educational alerts from two to one, at its discretion. *See id.*

162 *See id*. at 8.

163 *See id.* at 9–10.

164 *See id.* at 10.

165 *See id.* The subscriber also "agrees to instruct other users of the subscriber's account to cease infringing conduct, if any." *Id.*

166 *Id.* at 10–12 .

167 *See id.* at 11–12.

168 *See id.*

169 *See id.* at 12.

170 *See id.*

must be accompanied by some mitigation measure.[171] 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.[172] 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.[173] At every stage, the system will "reset" for the subscriber if twelve months pass without the receipt of an additional alert.[174]

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.[175] 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.[176] Overall costs of administration are split between the copyright owner representative and ISP groups.[177] At the individual case level, an appealing subscriber pays a thirty-five dollar filing fee, which may be waived at the discretion of AAA.[178] The filing fee is refundable if the subscriber prevails in his or her appeal.[179] The appeal process is designed to be "automated to the maximum extent practicable."[180]

Each appeal is decided by a single reviewer chosen by AAA from a panel of neutrals.[181] Reviewers must be lawyers, but they are not required to have the level of legal and case management

---

171 *See id.* at 12–13.
172 *See id*.
173 *See id.* at 13.
174 *See id.*
175 *See id.* at 14.
176 *See id.* at 26; Three Major Steps Press Release, *supra* note 141 (announcing that AAA will conduct the independent reviews).
177 *See* MOU, *supra* note 11, at 14.
178 *See id.* at 30.
179 *See id.* at 28.
180 *Id.* at 34.
181 *See id.* at 31.

experience that AAA arbitrators deciding other kinds of cases have.[182] 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.[183] By the terms of the MOU, this copyright expert must agree to receive input from copyright owners concerning what the prevailing legal principles are.[184]

A subscriber initiates an appeal by completing an online form wherein the subscriber asserts a defense or defenses to the allegations in the alert.[185] 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.[186] 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.[187] 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.[188] 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.[189] The

---

182 *See id.* at 33.

183 *See id.* at 35.

184 *See id.* at 35.

185 *See id.* at 29.

186 *See id.* at 26.

187 *See id.*; 17 U.S.C. §§ 107–122 (2006) (limitations on exclusive rights).

188 *See* MOU, *supra* note 11, at 26–28 (explaining the standard of review for each of the six defenses).

189 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, Technical Report No. UW-CSE-08-06-01, UNIV. OF WASH. (2008), *available at* http://dmca.cs.washington.edu/dmca_hotsec08.pdf.

copyright owner or its agent 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.[190] 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 was not found to be "fundamentally unreliable."[191] 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.[192]

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.[193] 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.[194] 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.[195] This de facto security obligation arises whether or not the

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*, N.Y. TIMES (Feb. 22, 2008, 10:50 pm), http://bits.blogs.nytimes.com/2008/02/22/google-says-ip-addresses-arent-personal.

190 MOU, *supra* note 11, at 5, 27.

191 *Id.* at 5, 28.

192 *See id.* at 5 (providing that a confidential "finding of inadequacy" shall be issued if the method of identification is found to be "fundamentally unreliable").

193 *See id.* at 27.

194 *See id.*

195 *See 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. *See id.*

subscriber has any contractual obligation to his or her ISP to secure his or her router.[196]

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.[197] 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.[198] This is the only circumstance in which a subscriber's identity may ever be disclosed to a copyright owner within the structure of CAS.[199] In all other cases, the subscriber's identity is known only to the ISP and the reviewer.[200]

The remaining defenses—*fair use* and *publication before 1923*—derive from specific provisions of the Copyright Act.[201] The merits of a subscriber's fair use defense are determined pursuant to prevailing legal principles as determined by CCI's approved expert.[202] 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.[203] Decisions about what constitutes a "substantially complete" copy of a work appear to be left to copyright owners.[204] The final ground for appeal—that the work

---

196 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, at *2 (S.D.N.Y. July 9, 2012); AF Holdings, LLC v. Doe, No. C 12–2049 PJH, 2012 WL 3835102, at *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).

197 *See* MOU, *supra* note 11, at 27.

198 *See id.* at 29.

199 *See id.* at 14.

200 *See id.* at 29.

201 *See* 17 U.S.C. § 107 (2006) (fair use); 17 U.S.C. §§ 302–304 (2006) (duration).

202 *See* MOU, *supra* note 11, at 35.

203 *See id.* at 6.

204 *See* LaFrance, *supra* note 140, 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.*

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. The burden of demonstrating publication before 1923 falls on the subscriber.[205] 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.

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).[206] 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.[207] The reviewer may request supplemental information from the copyright owner or the ISP if such information is needed to decide the appeal.[208] 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.[209] The entire appeal process is designed to be completed within ten days of the reviewer's receipt of a complete file and within about thirty days of the initiation of the appeal.[210] If the subscriber prevails, the copyright alert in question is invalidated.[211]

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: 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

---

205 *See* MOU, *supra* note 11, at 6.
206 *See id.* at 29.
207 *See id.* at 31–32.
208 *See id.* at 32.
209 *See id.* at 33.
210 *See id.* at 31–35 (prescribing deadlines for successive phases of the review process).
211 *See id.* at 28.

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[212] 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.[213] 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.

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.[214]

---

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

[213] 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.*

[214] *See* Bridy, *Graduated Response*, *supra* note 19, at 104–05 (discussing the various uses of deep packet inspection).

1. Suspension of Access

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.

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.[215] 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.[216]

The MOU permits but does not require participating ISPs to suspend access for subscribers reaching the fifth or sixth copyright alert.[217] 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

---

215 *See* Bridy, *Graduated Response*, *supra* note 19, at 126.

216 *See id.*

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

suspensions, excluding services like telephony, e-mail, and multi-channel video programming.[218] 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.[219]

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.[220] On this side of the Atlantic, filtering has been an open topic of conversation between corporate copyright owners and 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.[221]

---

[218] *See id.* at 12.

[219] *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).

[220] *See* HORTEN, *supra* note 33, at 49–51 (discussing the right to freedom of expression under European law); *id.* at 89 (quoting from copyright industry submissions to EU governmental entities in support of a filtering mandate for ISPs).

[221] *See* Brad Stone, *AT&T and Other I.S.P.'s May Be Getting Ready to Filter*, N.Y. 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).

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 technology. Copyright infringing speech is not protected under the First Amendment,[222] but separating it from protected speech as it whips through cyberspace in tiny packets is a very 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.[223] Whereas the fair use analysis is subtle, contextual, and standards-based, software engines for filtering are rule-based, and the tension between the two persists even as the state of the art advances.[224] 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.[225] Judges and

---

[222] *See, e.g.*, Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d 556, 562 (S.D.N.Y. 2004).

[223] *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).

[224] 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.*, Dan Burk & Julie Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001); Edward W. Felten, *A Skeptical View of DRM and Fair Use*, COMM. ACM, Apr. 2003, at 57; James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719, 1752–53 (2005).

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., *Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Solution for U.S. ISPs*, PUBLIC KNOWLEDGE 1, 4–5, 47–52, http://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf (arguing that no technology can ensure that fair use rights will be protected).

[225] *See* IFPI, *supra* note 17, at 22 (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* Rep. Lamar Smith, *Myth v. Fact: Stop Online Piracy Act*, U.S. House of Representatives Judiciary Comm., *available at* http://judiciary.house.gov/issues/Rogue%

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.[226] 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.[227] 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.[228]

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 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. This is a commendable if imprecise effort to accommodate fair use by treating transfers of partial copies as non-events.[229] On the whole, then, CAS should not be a major cause of

20Websites/011812_SOPA%20Myth%20vs%20Fact.pdf (last visited Nov. 16, 2012) (asserting without qualification that the website blocking provision in the Stop Online Piracy Act implicates no speech protected by the First Amendment).

[226] *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, 159 (2012) (detailing the public outcry in response to SOPA and PIPA).

[227] Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), 2011 ¶¶ 52–54, http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5311.

[228] *See id.* at ¶ 52.

[229] 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

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.[230] 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 U.S. 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.[231] Second, corporate copyright owners have been very successful at convincing courts and legislators that the right to go incognito online should not shield alleged infringers from liability.[232]

works are much more likely than partial copies to be infringing. *See* 17 U.S.C. § 107 (2006) (setting forth the fair use factors). The focus on substantially complete copies will likely lead to some degree of under-identification of infringing file transfers.

[230] *See id.* ¶ 84. 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.

[231] *See generally* CHRIS JAY HOOFNAGLE, EUROPEAN COMM'N DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SEC., COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS—COUNTRY STUDIES: UNITED STATES (2010) (providing an overview of data and privacy protections in the United States at federal and state levels), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1639161. 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).

[232] *See* 17 U.S.C. § 512(h) (2006) (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); Sony Music Entm't Inc. v. Does 1-40,

1. Surveillance

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.[233] Blocking can be done crudely on a 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.[234] 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."[235] More recently, Derek Bambauer cast it in Orwellian terms.[236] 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

326 F. Supp. 2d 556, 567 (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).

[233] 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. *Technology Overview*, AUDIBLE MAGIC, http://audiblemagic.com/technology.php (last visited Nov. 16, 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." *PacketShaper*, BLUE COAT, https://www.bluecoat.com/products/packetshaper (last visited Nov. 16, 2012).

[234] *See* KLAUS MOCHALSKI ET AL., IPOQUE, COPYRIGHT PROTECTION IN THE INTERNET (2009), *available at* 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).

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

[236] *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863 (2012).

for a dozen different ends—including copyright enforcement.[237] They do now, though, thanks to DPI.

Privacy scholars have questioned whether ISPs' use of DPI violates the Wiretap Act.[238] Despite its questionable legality, however, DPI has become standard operating procedure for ISPs for such purposes as congestion management and spam- and virus-filtering.[239] 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.[240] 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.[241] The Federal Communications Commission (FCC) sanctioned Comcast in 2008 for its use of DPI to manage

---

[237] *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1423–24, 1436 (2009) (discussing the unique position ISPs occupy in the economy of Internet surveillance).

[238] 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. *See 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 involved in any given online communication. *See id.*

[239] 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.

[240] *See* Bridy, *Graduated Response*, *supra* note 19, 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).

[241] *See* Bridy, *Graduated Response*, *supra* note 19, at 120–24 (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"); 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).

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.[242] 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.[243] Although those regulations will likely not survive judicial review, the exception they make for copyright enforcement highlights the extent to which the U.S. 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.[244] ISPs play no role in this type of self-help monitoring, which is sometimes referred to as

---

[242] *See* Comcast Corp. v. FCC, 600 F.3d 642, 644, 661 (D.C. Cir. 2010) (holding that the FCC lacks statutory authority to regulate the network management practices of broadband providers). Comcast was not using DPI for copyright enforcement purposes. *Id.* at 645.

[243] *See* 47 C.F.R. § 8.9 (2011) ("Nothing in this part prohibits reasonable efforts by a provider of broadband Internet access service to address copyright infringement or other unlawful activity."); *In the Matter of Preserving the Open Internet*, 25 FCC Rcd. 17905 (Federal Communications Commission) (2010) (FCC issues a final order establishing net neutrality rules); Brief for Appellant at 2, Verizon v. FCC, No. 11-1355, (D.C. Cir. 2012), 2012 WL 2561139 (seeking to invalidate net neutrality rules issued by the FCC in 2010).

[244] MarkMonitor, which acquired industry leader DtecNet in 2010, is now probably the largest provider in this space, but other firms, such as Peer Media Technologies, also offer P2P monitoring services. *See, e.g.*, Josh Halliday, *Copyright Tracking Firm DtecNet In Multinational Buyout*, THE GUARDIAN (Oct. 18, 2012, 6:29 AM), http://www.guardian.co.uk/technology/blog/2010/oct/18/copyright-dtecnet-markmonitor (describing DtechNet's market share at the time of acquisition); Robin Wauters, *MarkMonitor Acquires DTecNet to Combat Online Piracy*, TECH CRUNCH (Oct. 18, 2010), http:// techcrunch.com/2010/10/18/markmonitor-dtecnet (stating that MarkMonitor bought DtecNet, a global antipiracy company); *Notification Services*, PEER MEDIA TECHNOLOGIES, http://peermediatech.com/notification.html (last visited Nov. 16, 2012) (describing P2P and cyberlocker monitoring services).

"over-the-top" (OTT) surveillance because it operates at the Internet's application layer and not at the level of physical infrastructure.[245] 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.[246] OTT surveillance provides the evidentiary basis for sanctions in the French and Irish implementations of graduated response, and corporate rights owners in the U.S. have relied on it since the early 2000s, when they began monitoring P2P networks in conjunction with their litigation campaign against individual file sharers.[247] 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.[248]

Under the MOU, copyright owners take the OTT approach to monitoring, which is significantly less invasive of user privacy than DPI-based surveillance.[249] While Trisha Meyer and Leo Van Audenhove have argued rightly that graduated response contributes to the normalization of surveillance on the Internet,[250]

---

[245] *See* Mueller et al., *supra* note 240, 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*, IEEE COMMC'NS MAGAZINE, Aug. 2009, at 107, 107 (explaining that P2P applications "discover a route to each other through an overlay network with little knowledge of the underlying network topology").

[246] *See, e.g.*, Anirban Banerjee et al., *The P2P War: Someone Is Monitoring Your Activities!*, 52 J. COMPUTER NETWORKS 1272, 1272–73 (2008) (explaining how to identify and avoid the "fake users" employed by the RIAA and the MPAA on P2P networks).

[247] *See* Annemarie Bridy, *Why Pirates (Still) Won't Behave: Regulating P2P in the Decade After Napster*, 40 RUTGERS L. J. 565, 590–96 (2009) [hereinafter Bridy, *Pirates*] (discussing the surveillance program on which the RIAA's litigation campaign relied to produce evidence of P2P infringements).

[248] *See, e.g.*, *About Copyright Notices*, RIAA, https://www.riaa.com/toolsforparents.php?content_selector=resources-music-copyright-notices (last visited Nov. 16, 2012) (emphasizing that P2P file sharers are not anonymous).

[249] *See* Mueller et al., *supra* note 240, at 360 (pointing out that the MOU relies on OTT methods for surveillance rather than on DPI).

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

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.[251] 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.[252] Users who want to engage in unmonitored P2P transactions can do so via password-secured networks or virtual private networks (VPNs), and OTT monitoring by copyright owners has almost certainly driven a percentage of P2P traffic underground.[253] If copyright owners were to attempt to monitor online activity in such secured environments, the threat to privacy 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.[254]

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

(arguing that "graduated response . . . allows the move towards a permanent surveillance of citizens' conduct on the Internet").

[251] 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 (H. Ct.) (Ir.).

[252] In one study, 100% of peers participating in observed P2P networks over a ninety-day period between January and March 2006 made contact with one or more fake users. *See* Banerjee et al., *supra* note 246, at 1272.

[253] TorrentFreak, a site dedicated to P2P file sharing, has rated VPN providers based on the degree to which they protect user anonymity in the face of third party requests for identifying information. *See Which VPN Providers Really Take Anonymity Seriously?*, TORRENTFREAK (Oct. 7, 2011), http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007 (discussing the results of the survey).

[254] 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 v. Data Protection Comm'r, [2012] IEHC 264, ¶ 7.2 (H. Ct.) (Ir.) (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).

subscriber, even after the CAS protocol has run its course for subscribers who are repeat recipients.[255] 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.[256] 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 twelve months without receiving an additional alert.[257] To assure protection of consumer privacy, expungement on reset should be mandatory rather than permissive.

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 U.S. 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.[258] 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

---

[255] *See* MOU, *supra* note 111, 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").

[256] *See id.* 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.").

[257] *See id.* at 13.

[258] *See, e.g.*, Virgin Records Am., Inc. v. Doe, No. 5:08-CV-389-D, 2009 WL 700207, at *2 (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).

then issuing subpoenas to their ISPs.[259] 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.[260]

With respect to the preservation of anonymity, the notice system at the core of graduated response does not require disclosure of subscribers' 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.[261] 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.[262]

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

---

[259] *See, e.g.*, UMG Recordings, Inc. v. Does, 64 Fed. R. Serv. 3d 305, *1 (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).

[260] 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) (2006) (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* RIAA v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1229 (D.C. Cir. 2003).

[261] *See* MOU, *supra* note 11, at 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").

[262] *See id.* at 32.

comprehensive and surreptitious than ISP-based surveillance, which would be a truly 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.[263] 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.[264] 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.[265] 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.

---

[263] *See* Bridy, *supra* note 3, at 720–25 (arguing that John Doe litigation is a "dysfunctional workaround" for the DMCA's failure to scale for P2P file sharing).

[264] *See* Bridy, *supra* note 3, at 736 (asserting that graduated response systems must be designed to honor the competing values of efficiency and fairness); LaFrance, *supra* note 140, at 175 (finding that CAS "comes up short in several respects" when viewed through the lens of 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, *supra* note 18, at 1419–20 (arguing that a graduated response system must respect the rule of law and the norms of fairness and legitimacy).

[265] *See supra* note 75 and accompanying text.

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.[266] 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.[267] 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, with respect to both the capture of IP addresses and the identification of copyrighted content.[268] 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.[269] 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.[270] Such treatment was criticized in *Corbis Corp. v. Amazon.com*, a case interpreting the repeat infringer provision of the DMCA.[271]

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 until proven otherwise. In keeping with that principle, Peter Yu has called for a focus in graduated response on *proven* infringers as opposed to *alleged* infringers.[272] As I have argued

---

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

267 *See* MOU, *supra* note 11, at 27–28 (setting forth the technical requirements of CAS).

268 *See id.*

269 *See id.*

270 *See id.* at 28.

271 *See* Corbis Corp. v. Amazon.com, 351 F. Supp. 2d 1090, 1108–09 (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 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).

272 *See* Yu, *supra* note 18, at 1418 (emphasis in original).

elsewhere, however, litigation doesn't scale well for enforcing copyrights against P2P file sharers.[273] 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. 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),[274] 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 above in Part III.B, for any subscriber who wants to contest the accuracy

273 *See* Bridy, *supra* note 3, at 719–25.

274 *See id.*

or validity of one or more alerts after the fact. The imposition of a mitigation measure is stayed pending the outcome of review.[275] 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 defenses, along with supporting facts.[276] In keeping with the efficiency imperative, there are no hearings, and there is no discovery.[277] 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.[278] And the subscriber's right to elect a traditional judicial forum, where hearings and discovery are the rule, is not foreclosed.[279]

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.[280] 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.[281] The

---

[275] *See* MOU, *supra* note 11, at 30.

[276] *See id.* at 31 (specifying the contents of the Application to Commence Independent Review (ACIR) package).

[277] *See id.* at 33.

[278] *See id*. at 32.

[279] *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").

[280] *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).

[281] *See id.* at 524 (asserting that an arbitrator's incentive to secure future business from a repeat customer is corrosive of impartiality). Professor LaFrance has questioned whether the CAS independent review process will inevitably suffer from the problem of

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.[282] 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.[283] Notwithstanding that fact, preserving the option of litigation allows subscribers to get full procedural due process if they want it.

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 principles as determined by United States federal courts" and interpreted by the AAA-commissioned, CCI-board-approved independent expert.[284] 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

"embedded neutrals." LaFrance, *supra* note 140, at 183 (citing a study by Nancy Welsh on bias in arbitration).

[282] *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).

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

[284] MOU, *supra* note 11, at 35.

principles."[285] 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.[286] When potentially biased interpretations of the law govern an arbitral process potentially subject to repeat-player bias, there is good reason to doubt 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."[287] 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.[288] If such statements are among the legal principles that will govern appeals under CAS,

---

[285] *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").

[286] *See id.* (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").

[287] *The Law*, RIAA, https://www.riaa.com/physicalpiracy.php?content_selector=piracy_online_the_law (last visited Nov. 16, 2012).

[288] 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. *See, e.g.*, Metro-Goldwyn-Mayer Studios Inc., v. Grokster Ltd., 545 U.S. 913, 919 (2005) ("[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."); A&M Records Inc., v. Napster Inc., 239 F.3d 1004, 1027 (9th Cir. 2001) ("Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index."); Artista Records LLC v. Lime Group LLC, 784 F. Supp. 2d 398, 436–37 (S.D.N.Y. 2011) (holding LimeWire liable for inducing copyright infringement).

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.[289] 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 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 sixteen sections—107 through 122—enumerate a wide range of limitations that are crucial for maintaining a balanced copyright system.[290] 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.[291]

---

[289] *See* MOU, *supra* note 11, 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. *See id.*

[290] *Id.*

[291] *See* 17 U.S.C. § 107 (2006) (fair use); 17 U.S.C. §§ 302–304 (2006) (duration).

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 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.[292] 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.

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.[293]

---

[292] *See* Pamela Samuelson, *Reforming Copyright Is Possible*, CHRON. HIGHER EDUC. (D.C.), July 9, 2012, *available at* http://chronicle.com/article/Reforming-Copyright-Is/132751 (listing the various ways that works can fall into the public domain).

[293] Mary LaFrance has also criticized CAS for placing limits on available defenses. *See* LaFrance, *supra* note 13940, at 175–76.

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."[294] 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.[295] Three strikes protocols that culminate in disconnection have been found by the EU Data Protection Supervisor to violate the principle of proportionality,[296] although the Irish High Court reached the opposite conclusion in the Eircom case.[297]

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.

---

294 Directive 2001/29, art. 8, 2001 O.J. (L 167) 10, 18 (EC).

295 *See* Tor-Inge Harbo, *The Function of the Proportionality Principle in EU Law*, 16 EURO. L.J. 158, 165 (2010) ("According to the conventional understanding of the proportionality principle, it consists of three tests applied to the allegedly infringing measure, respectively the suitability, the necessity and the proportionality *stricto sensu* test.").

296 *See Opinion of the European Data Protection Supervisor*, *supra* note 64, at 5.

297 *See* EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 30 (H. Ct.) (Ir.) ("There is nothing disproportionate . . . about cutting off internet access because of three infringements of copyright.").

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.[298] 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.[299] 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 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

---

[298] *See* Bridy, *Pirates*, *supra* note 247, at 604 (citing a study by the Pew Internet Project).

[299] *See* Bridy, *supra* note 3, at 716–25.

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.[300] 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.

[300] The controversial—and ultimately abandoned—Stop Online Piracy Act contained a provision requiring ISPs to block access to "foreign infringing 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. § 102(c)(2)(A)(i) (2011).

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, implementation, and outcomes. Across these domains, an endemic lack of disclosure undermines the credibility of the system and the public's confidence in it.

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.[301] 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. 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."[302]

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

---

[301] *See* Bridy, *ACTA*, *supra* note 10, at 576–77 (highlighting the public law effects of the EMI-Eircom settlement and the ways in which such private settlements undermine consumer protection).

[302] LaFrance, *supra* note 140, at 167.

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 substantive rules that will be applied in the independent review program.

CAS has been criticized by academics and commentators in the blogosphere for the lack of transparency surrounding its implementation.[303] On the heels of this criticism, CCI released Stroz Friedberg's "independent assessment" of the methodologies that will be used by participating copyright owners to identify infringing files and alleged infringers.[304] The assessment, many details of which were redacted in the released version, includes several recommendations for process improvement, including the development of an auditing framework.[305] The assessment predictably does not include any finding of technical inadequacy and concludes that the technology underlying CAS is "well developed and robust."[306]

It appears from the release of the Stroz Friedberg assessment that CCI intends to be more forthcoming and transparent than the MOU actually requires. The fact remains, however, that secrecy is

---

[303] *See, e.g.*, *id.* at 166; *"Six Strikes" Anti-Piracy Scheme Overly Secret and Unfair, Says Professor*, TORRENTFREAK (Sept. 17, 2012), http://torrentfreak.com/six-strikes-anti-piracy-scheme-overly-secret-and-unfair-says-professor-120917 (quoting at length from a preliminary draft of this Article published on SSRN).

[304] *See* INDEPENDENT EXPERT ASSESSMENT OF MARKMONITOR ANTIPIRACY METHODOLOGIES [REDACTED], Stroz Friedberg, Nov. 1, 2012, http://www.copyrightinformation.org/sites/default/files/Independent%20Expert%20Assessment.Content.CCI_.Redacted.pdf.

[305] *See id.* at 2,11.

[306] *See id.* at 2.

the rule in the agreement, and the independent experts hired to ensure the technical integrity of the system may not disclose any information about the copyright owner methodologies—even to the CCI advisory board—without express written consent.[307] The secrecy to which the independent technical expert is bound is a genuine cause for concern given that a copyright owner can decline to adopt expert recommendations without breaching the MOU 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 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 worry 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.[308] 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,

---

[307] *See* MOU, *supra* note 11, at 5 ("[T]he 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.").

[308] *See supra* Part IV.C.

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.[309] 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.[310] 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.[311] Using that 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.[312] 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 is unknown whether any of it will flow out to the public in any form. Nothing in the MOU suggests that public disclosure about outcomes is part of the program.

On the contrary, the secrecy requirements in the MOU that cover the technical infrastructure of CAS also cover data

---

309 *See* MOU, *supra* note 11, at 18 (stating that the CCI uses reports to assess "the number of ISP notices received and the number of corresponding Copyright Alerts sent," which are part of both content owners' and ISPs' obligations).

310 *See id.* at 14–15.

311 *See id.* at 18.

312 *See id.* at 18–19.

disclosure concerning measured outcomes. The MOU requires CCI to "maintain any reports or other information 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."[313] The MOU goes so far as to require CCI to seek a protective order from a court if information it has received from a party becomes subject to a subpoena or other legal process.[314]

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

CCI expects CAS to launch across participating ISPs sometime in early 2013—a delay over previous projections.[315] When the launch does finally occur, assuming that it will, millions of Americans will become subject to 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

313 *Id.* at 19.

314 *See id.*

315 *See* Jill Lesser, *Dotting our "I"s*, Ctr. for Copyright Information, Nov. 28, 2012, http://www.copyrightinformation.org/node/714 (announcing a delay in the expected launch date for CAS so that CCI can "be sure that all of [its] 'I's are dotted and 'T's crossed before any company begins sending alerts").

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.