Florida Law Review

Volume 62 | Issue 5 Article 6

December 2010

The Graduated Response

Peter K. Yu

THE GRADUATED RESPONSE

Peter K. Yu[*]

 Kern Family Chair in Intellectual Property Law & Director, Intellectual Property Law Center, Drake University Law School; Wenlan Scholar Chair Professor, Zhongnan University of Economics and Law. An earlier version of this Article was presented at the 10th Intellectual Property Scholars Conference at Boalt Hall School of Law, University of California at Berkeley, the "Internet Expression" Symposium at Widener University School of Law—Harrisburg, the 2010 Intellectual Property Scholars Roundtable at Drake University Law School and as a lecture at Zhongnan University of Economics and Law. The Author would like to thank Tonya Evans for her kind invitations and hospitality and to Annemarie Bridy, Jeremy de Beer, Rob Frieden, Eric Goldman, Sonia Katyal, Jennifer Rothman, David Simon, Ned Snow, Jennifer Urban, and the participants of these events for their valuable comments and suggestions. He is also grateful to Megan Snyder for excellent research and editorial assistance.

INTRODUCTION

In the past few years, the entertainment industry has deployed aggressive tactics toward individual end-users, Internet service providers (ISPs), and other third parties.[1] While these tactics have had only mixed results and have been heavily criticized by policymakers, civil liberties groups, consumer advocates, and academic commentators, the industry continues its desperate search for an effective and more publicly acceptable solution to address massive online copyright infringement.

One of the latest proposals that the industry has been exploring is the so-called "graduated response" system. Similar to other "three strikes and you're out" systems that are commonly found in the United States, the graduated response system provides an alternative enforcement mechanism,[2] through which ISPs can take a wide variety of actions after giving users two warnings[3] about their potentially illegal online file-sharing activities. These actions include, among others, suspension and termination of service, capping of bandwidth, and blocking of sites, portals, and protocols.

In December 2008, the Recording Industry Association of America (RIAA) made a formal public announcement of its change of focus toward greater cooperation with ISPs.[4] This new collaborative effort seeks to replace the highly unpopular lawsuits the industry has filed against individual file-sharers in the past five years. To strengthen their legal positions and to induce greater cooperation from ISPs, some industry groups have suggested that the graduated response system had already been built into the framework under the Digital Millennium Copyright Act of 1998 (DMCA)[5]—a proposition that ISPs, civil liberties groups, consumer advocates, and academic commentators have vehemently rejected.[6]

---

1. For discussions of the aggressive and ill-advised tactics employed by the U.S. entertainment industry in the past few years, see generally Peter K. Yu, *The Escalating Copyright Wars*, 32 HOFSTRA L. REV. 907, 910–23 (2004); Peter K. Yu, *P2P and the Future of Private Copying*, 76 U. COLO. L. REV. 653, 658–98 (2005) [hereinafter Yu, *P2P and the Future*].

2. *See* Alain Strowel, *Internet Piracy as a Wake-up Call for Copyright Law Makers—Is the "Graduated Response" a Good Reply?*, 1 WIPO J. 75, 77–80 (2009).

3. The number of warnings will vary in accordance with the type of graduated response system. Two warnings are used here to reflect the commonly discussed "three strikes" model.

4. *See* Nate Anderson, *RIAA Graduated Response Plan: Q&A with Cary Sherman*, ARS TECHNICA, Dec. 21, 2008, http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars; Steve Knopper, *RIAA's Gaze Turns from Users to ISPs in Piracy Fight*, ROLLING STONE, Dec. 19, 2008, http://www.rollingstone.com/music/news/14844/94542.

5. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

6. *Compare* Eric Smith, President, Int'l Intellectual Prop. Alliance, Remarks at the American University Washington College of Law Symposium: Beyond TRIPS: The Current Evolving Law of International Enforcement of Intellectual Property (Nov. 5, 2009), *available at* http://media.wcl.american.edu/Mediasite/SilverlightPlayer/Default.aspx?peid=33d4b6cefcd44ea6893d2f603661b6d2, *with* Gigi Sohn, President, Pub. Knowledge, Remarks at the American

The push for the graduated response system came at a very interesting time when the Obama administration was actively pushing for greater expansion of Internet service in underserved and unserved areas, especially those in rural America.[7] The recently adopted government stimulus package, for example, has earmarked more than $7 billion for broadband deployment.[8] The demand for the development of a graduated response system also came amidst a raging debate concerning the country's future telecommunications policy, implicating such issues as the principle of network neutrality[9] and the role of deep packet inspection[10] in network

---

University Washington College of Law Symposium: Beyond TRIPS: The Current Evolving Law of International Enforcement of Intellectual Property (Nov. 5, 2009), *available at* http://media.wcl.american.edu/Mediasite/SilverlightPlayer/Default.aspx?peid=33d4b6cefcd44ea6893d2f603661b6d2. *See also* discussion *infra* Part II.

7. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 128, 512 (providing $4.7 billion in the Broadband Technology Opportunities Program to promote and improve access to broadband service in underserved and unserved areas).

8. *See* Stephanie Condon, *Stimulus Bill Includes $7.2 Billion for Broadband*, CNET NEWS, Feb. 17, 2009, http://news.cnet.com/8301-13578_3-10165726-38.html.

9. For articles engaging in the network neutrality debate, see generally Barbara A. Cherry, *Misusing Network Neutrality to Eliminate Common Carriage Threatens Free Speech and the Postal System*, 33 N. KY. L. REV. 483 (2006); Susan P. Crawford, *Network Rules*, LAW & CONTEMP. PROBS., Spring 2007, at 51; Rob Frieden, *Network Neutrality or Bias?—Handicapping the Odds for a Tiered and Branded Internet*, 29 HASTINGS COMM. & ENT. L.J. 171 (2007); Brett M. Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS J. 383 (2007); Lawrence Lessig, *In Support of Network Neutrality*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 185 (2007); Howard A. Shelanski, *Network Neutrality: Regulating with More Questions than Answers*, 6 J. ON TELECOMM. & HIGH TECH. L. 23 (2007); Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. ON TELECOMM. & HIGH TECH. L. 329 (2007); Philip J. Weiser, *Toward a Next Generation Regulatory Strategy*, 35 LOY. U. CHI. L.J. 41 (2003); Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141 (2003); Tim Wu, *The Broadband Debate: A User's Guide*, 3 J. ON TELECOMM. & HIGH TECH. L. 69 (2004); Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1 (2005); Christopher S. Yoo, *Network Neutrality, Consumers, and Innovation*, 2008 U. CHI. LEGAL F. 179; Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847 (2006).

10. As Professor Kevin Werbach described:

> Deep packet inspection uses specialized high-speed hardware and software that can identify packets in real-time. A service provider could use deep packet inspection to distinguish peer-to-peer traffic, or even just traffic from a single peer-to-peer file-sharing application, and either block it or reduce its available bandwidth. Without deep packet inspection, service providers and others could only resort to crude application-level techniques, such as cutting off all streaming video clips using standard formats after a certain time. Deep packet inspection allows true logical-layer control based on ownership of the physical layer.
>
> Service providers may deploy deep packet inspection gear for several reasons. With peer-to-peer applications representing more than half of the total traffic on the Internet, broadband service providers have incentives to limit those applications' bandwidth utilization. Separately, the FCC's CALEA [Communications Assistance to Law Enforcement Act] proposal would require

management and intellectual property protection.[11] In March 2010, the Federal Communications Commission (FCC) announced its intent to undertake a major overhaul of the nation's broadband policy.[12] Such an overhaul aims to dramatically increase Internet speeds (including those of online uploads and downloads) while revolutionizing the way Americans use the medium.

If the timing of these developments is not interesting enough, the ongoing debate concerning the graduated response system parallels similar debates across the world. In May 2009, for example, France adopted the *Loi favorisant la diffusion et la protection de la création sur internet*, which established a new administrative body called HADOPI to impose, among other measures, suspension or termination of Internet service.[13] Although the French Constitutional Council struck down part of the law as unconstitutional,[14] the legislature quickly adopted a replacement law that introduced an additional judicial process.[15] With the blessing of the Constitutional Council, this new law has now entered into effect.

In addition to France, similar laws and policies have been adopted, considered, or rejected by Australia, Germany, Hong Kong, the

> network owners to facilitate wiretapping of VoIP calls. Deep packet inspection could make that easier to accomplish, by isolating VoIP traffic flows. Cisco recently paid $200 million to acquire P-Cube, a deep packet inspection startup, indicating the level of interest in the potential market for such technology.

Kevin Werbach, *Breaking the Ice: Rethinking Telecommunications Law for the Digital Age*, 4 J. ON TELECOMM. & HIGH TECH. L. 59, 92–93 (2005).

11. *See* Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 633, 652 (2008) ("[Deep] packet inspection also provides ISPs with a greater ability to determine whether the traffic they carry respects all intellectual property rights of the content creator. In other words, packet sniffing provides the means for ISPs to determine whether their network has become a medium for the unlawful transport of files to recipients lacking lawful authority to consume, copy, and share intellectual property.").

12. John Poirier & Sinead Carew, *U.S. to Roll Out Major Broadband Policy*, REUTERS, Mar. 14, 2010, http://www.reuters.com/article/idUSTRE62D0ZX20100314.

13. LOI n° 2009–669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Law No. 2009–669 of June 12, 2009 to Promote the Dissemination and Protection of Creation on the Internet), Journal Officiel de la République Française [J.O.] [Official Gazette of France], June 12, 2009, p. 9666, *available at* http://legifrance.gouv.fr/affichTexte.do;jsessionid=69C250441C04AFAED3A3EC46276A39BD.tpdjo14v_1?cidTexte=JORFTEXT000020735432&categorieLien=id. "'HADOPI' stands for the 'High Authority for the Diffusion of Works ('Oeuvres' in French) and the Protection of Rights on the Internet.'" Strowel, *supra* note 2, at 79 n.12.

14. CC decision no. 2009–580DC, July 10, 2009, J.O. 9675, *available at* http://www.conseil-constitutionnel.fr/decision.42666.html; *see also* Strowel, *supra* note 2, at 79–84.

15. LOI n° 2009–669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Law No. 2009–669 of June 12, 2009 to Promote the Dissemination and Protection of Creation on the Internet) (amended Oct. 28, 2009), *available at* http://legifrance.gouv.fr/affichTexte.do;jsessionid=69C250441C04AFAED3A3EC46276A39BD.tpdjo14v_1?cidTexte=LEGITEXT000020736830&dateTexte=20100314; *see also* Strowel, *supra* note 2, at 80.

Netherlands, New Zealand, South Korea, Sweden, Taiwan, and the United Kingdom.[16] Thus far, proposals for the development of a graduated response system have been rejected by Germany, Hong Kong, Spain, and Sweden as well as the European Parliament.[17] As Sweden noted when it rejected the system in March 2008: "[C]opyright owners should 'not use the copyright laws to defend old business models' but should rather offer legitimate services."[18] Likewise, in the digital copyright reform proposal recently submitted to the Legislative Council, the Hong Kong government stated that the present is "not an opportune time to consider introducing such a system in Hong Kong, especially when its implications are yet to be fully tested in overseas jurisdictions."[19]

In February 2010, European policymakers expressed their reluctance to include the graduated response system in the Anti-Counterfeiting Trade Agreement (ACTA),[20] a controversial plurilateral intellectual property agreement that is currently under negotiation.[21] As a spokesperson for the European Commission's trade commissioner declared:

> We are not supporting and will not accept that an eventual Acta agreement creates an obligation to disconnect people from the internet because of illegal downloads . . . . The 'three-strike rule' or graduated response systems are not compulsory in Europe. Different EU countries have different approaches, and we want to keep this flexibility.[22]

A month later, the European Parliament adopted a resolution, taking "a strong stand specifically against the adoption of 'three strikes' rules against IP violators."[23] This resolution resonates well with the Parliament's earlier amendment to its telecommunications reform package, which declares:

---

16. For a discussion of the emerging global trend toward more active prevention of copyright infringement by intermediaries, see generally Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009).

17. *See* WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS 14 (2009); Howell Llewellyn, *'Three-Strikes' Off Anti-Piracy Agenda in Spain*, BILLBOARD.BIZ, June 22, 2009, http://www.billboard.biz/bbbiz/content_display/industry/e3i8071e0d9c25cb6b876d3771fb7e3d102; Peter Ollier, *Hong Kong Rejects Three-Strikes Copyright Rule*, MANAGING IP, Nov. 23, 2009, http://www.managingip.com/Article/2344270/Hong-Kong-rejects-three-strikes-copyright-rule.html (subscription required). Although these jurisdictions have rejected the graduated response system, they can always reconsider the rejected proposal. *See, e.g.*, *infra* note 19 and accompanying text.

18. PATRY, *supra* note 17.

19. COMMERCE & ECON. DEV. BUREAU, H.K. SPECIAL ADMIN. REGION GOVERNMENT, PROPOSALS FOR STRENGTHENING COPYRIGHT PROTECTION IN THE DIGITAL ENVIRONMENT 6 (2009) [hereinafter HKSAR LEGCO PROPOSALS].

20. David Meyer, *Europe 'Will Not Accept' Three Strikes in ACTA Treaty*, ZDNET, Feb. 26, 2010, http://news.zdnet.co.uk/communications/0,1000000085,40057434,00.htm.

21. For a detailed discussion of the origins and ongoing negotiation of ACTA, see generally Peter K. Yu, *Six Secret (and Now Open) Fears of ACTA*, 64 SMU L. REV. (forthcoming 2011), *available at* http://ssrn.com/abstract=1624813.

22. Meyer, *supra* note 20.

23. Scott M. Fulton, III, *Strongest Condemnation Yet of Anti-Counterfeiting, 'Three Strikes' from EU*, BETANEWS, Mar. 10, 2010, http://www.betanews.com/article/Strongest-condemnation-yet-

> "Any of the[] measures [taken by Member States] regarding end-users' access to or use of services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may *only* be imposed if they are *appropriate, proportionate and necessary within a democratic society*, and their implementation shall be subject *to adequate procedural safeguards* in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law, including *effective judicial protection* and *due process*."[24]

Given the ongoing debate concerning the expediency of the graduated response system and the system's larger implications for broader Internet and telecommunications policies, whether U.S. policymakers or industries embrace the system is likely to have serious worldwide ramifications. To help us better understand the effectiveness of the graduated response system in addressing massive online copyright infringement, Part I of this Article examines the benefits and drawbacks of the system. This Part focuses on three groups of stakeholders in the copyright system: copyright holders, ISPs, and Internet users. Part II evaluates the claims of some industry representatives that the graduated response system has already been built into the so-called DMCA framework. This Part explores what Congress intended to cover when it enacted a statute requiring ISPs to adopt and reasonably implement a policy for terminating the service of repeat infringers and to inform their users of such a policy. It underscores the important distinction between *alleged* and *proven* repeat infringers. Part III introduces three thought experiments to highlight the problems and unintended consequences the graduated response system would bring

---

of-anticounterfeiting-three-strikes-from-EU/1268242864; *see also* Michael Geist, *Joint European Parliament ACTA Transparency Resolution Tabled*, http://www.michaelgeist.ca/content/view/4848/125/ (Mar. 9, 2010) (providing the draft resolution that states that "in order to respect fundamental rights such as freedom of expression and the right to privacy, with full respect for subsidiarity, the proposed Agreement must refrain from imposing any so called 'three strikes' procedures, in full respect of the decision of Parliament on article 1.1b in the (amending) Directive 2009/140/EC that calls to insert a new para 3 a to article 1 Directive 2002/21/EC on the matter of 'three strikes'").

24. Press Release, European Union, Agreement on EU Telecoms Reform Paves Way for Stronger Consumer Rights, an Open Internet, a Single European Telecoms Market and High-speed Internet Connections for All Citizens, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491 (Nov. 5, 2009) (quoting Article 1(3)(a) of the new Framework Directive) (emphasis in original modified). As Guy Bono, the drafter of the amendment, stated, "We do not play like that with individual liberties. The French government should review its [graduated response system]!" *Id.* Christofer Fjellner, a Swedish member of the European Parliament, concurred: "'What's important about this decision is that now it's clear that you can't force [internet service] providers to ban people from the internet without a legal process' . . . ." David Landes, *Sweden Welcomes EU Telecoms Vote*, THE LOCAL (Sweden), Sept. 24, 2008, http://www.thelocal.se/14548/20080924/ (quoting Christofer Fjellner, a Swedish member of the European Parliament).

about. These experiments focus on (1) the emergence and proliferation of user-generated content, (2) the protection of free speech and free press, and (3) the retention of the fair use privilege in copyright law. Part IV concludes by outlining seven basic principles that policymakers need to take into account if they choose to institute a graduated response system despite its many shortcomings.

I. GRADUATED RESPONSE SYSTEM

The graduated response system began as a "three strikes" system. It seeks to strike the middle ground by providing sufficient warning to Internet users who might have engaged in illegal online file-sharing activities while at the same time protecting the interests of copyright holders, such as those in the publishing, recording, movie, software, and game industries. Although similar "three strikes" laws and policies have been widely used in the United States—and the phrase "three strikes" was derived from America's most favorite pastime—such a moniker achieves neither easy recognition nor wide acceptance abroad. At times, the moniker has brought with it some negative connotations, such as those associated with physical assault and gun violence.[25]

A more accurate term, the "graduated response," is therefore preferred and has since been used in lieu of "three strikes," even though policymakers and industry experts continue to use the original term.[26] Compared to "three strikes," the term "graduated response" reflects better the fact that ISPs can take action before a user has been "struck" three times. It also recognizes the wide flexibility ISPs have in determining the appropriate sanctions based on the number and type of warnings given to users and the severity of their potentially infringing activities.[27]

---

25. *See* Nate Anderson, *IFPI: "Three Strikes" Efforts Hit Worldwide Home Run*, ARS TECHNICA, Aug. 19, 2008, http://arstechnica.com/tech-policy/news/2008/08/ifpi-three-strikes-efforts-hit-worldwide-home-run.ars (noting the observation of Shira Perlmutter, executive vice president of global legal policy for the International Federation of the Phonographic Industry, that "many Europeans at first took 'three strikes' to refer to physical assault rather than to baseball's 'three strikes and you're out'"); Jim Burger, Filtering & Graduated Response Against Online Infringers, http://www.dvd-intelligence.com/features/feature.php?feature=105 (last visited Sept. 18, 2010) ("Although one of its nicknames derives from American baseball, '*réponse graduée*' is a more appropriate name for a proposal whose most vocal and successful advocates are in France.").

26. Some Commonwealth jurisdictions have also described the system as "notice and termination." *See, e.g.*, Michael Geist, The Liberal Roundtable on the Digital Economy, http://www.michaelgeist.ca/content/view/4787/125/ (Feb. 11, 2010); Andrew Colley, *AFACT Opposes IIA's Intervention in iiNet Case*, AUSTRALIAN IT, Nov. 25, 2009, http://www.theaustralian.com.au/australian-it/afact-opposes-iias-intervention-in-iinet-case/story-e6frgakx-1225803692007.

27. As James Gannon observed:

> [T]he term ["three-strikes" laws] is misleading since the nature of sanctions imposed on repeat infringers varies to a great extent between the different schemes proposed. A better term to describe these initiatives is a "graduated

Even more problematically, as Michael Weinberg, a staff attorney of Public Knowledge, reminded us:

> Three Strikes is not just a misnomer because the number of strikes is wrong. It is also a misnomer because of the consequences it implies. In baseball, when you strike out the game goes on. You will probably get another chance to bat. You also get to keep playing in the field.[28]

Under the graduated response system, a repeat infringer may not have another chance to bat—at least not for a while. Nor may he or she retain the ability to "keep playing in the field."

Notwithstanding the use of this new and more appropriate moniker, commentators have questioned whether the term "graduated response" fully reflects the highly problematic nature of the system. Noted author William Patry, for example, declared in his new book, *Moral Panics and the Copyright Wars*: "The term graduated response should be replaced with the more accurate term 'digital guillotine,' reflecting its killing of a critical way people connect with the world and in some cases, eliminating their ability to make a living."[29] The term "digital guillotine" has also been used by the media—in particular, the French press—as well as civil liberties groups.[30]

To better understand the graduated response system—or this dreadful digital guillotine—this Part discusses the strengths and weaknesses of the system. While this system undoubtedly contains significant benefits and may provide copyright holders with a new weapon to combat massive online copyright infringement, the system, unfortunately, also has a number of major shortcomings that will raise significant concerns both within and without the intellectual property arena.

A. *Benefits*

The graduated response system provides benefits to three groups of stakeholders in the copyright system: copyright holders, ISPs, and those

---

> response" system. Essentially, the ISP issues a series of escalating warnings and sanctions to subscribers who persist in pirating content over the Internet, culminating in the termination of the subscriber's account with the ISP after a number of warnings have been ignored.

James Gannon, Graduated Response Systems, http://www.iposgoode.ca/2009/04/graduated-response-initiatives/ (Apr. 13, 2009).

28. Michael Weinberg, Three Strikes, Exile, and Judge Dredd, http://www.publicknowledge.org/node/2877 (Feb. 1, 2010).

29. PATRY, *supra* note 17, at 14.

30. *See, e.g.*, Fred von Lohmann, RIAA v. The People Turns from Lawsuits to 3 Strikes, http://www.eff.org/deeplinks/2008/12/riaa-v-people-turns-lawsuits-3-strikes (Dec. 19, 2008); Will France Introduce the Digital Guillotine in Europe?, http://www.laquadrature.net/en/enditorial-will-france-introduce-digital-guillotine-europe (Apr. 23, 2008).

Internet users who do not participate in illegal file-sharing activities. This section discusses each benefit in turn.

1. Copyright Holders

The graduated response system can serve as an effective deterrent.[31] Because school- and college-age Internet users highly value their Internet connection—sometimes more so than the money they, and often their parents, dole out to pay for the legal settlement with the entertainment industry—such a system is likely to have a strong deterrent effect. To some extent, the threat of Internet disconnection is similar to, and as effective as, the threat of suspension of a driver's license for drunk driving. Indeed, the prospect of losing one's Internet connection, and the attendant embarrassment and social isolation, may instill substantial fear among high school and college students.[32] In the United Kingdom, for example, "a test of the graduated response system showed that 70 percent of customers stopped infringing in the six-month period after receiving the first notice, with a further 16 percent stopping after the second notice."[33]

The graduated response system can also help exact retribution for the infringers' wrongful conduct. By encouraging one to respect the intellectual assets of others, the system helps foster respect for the rule of law and the legal rights of society's creative citizens. If a sufficient number of people find the system legitimate and socially desirable, that system, in the long run, will also help restore respect to copyright law, the respect of which has drastically eroded since the emergence of Napster, Grokster, and other file-sharing services.

In addition, as shown by the copyright holders' long and unsuccessful fight against online file-sharers, the graduated response system may be a necessary prophylactic measure. That system may also be effective for at least a couple of reasons. First, by doling out penalties, the system creates a disincentive for those Internet users who make unauthorized downloads of copyrighted materials without thinking about legal consequences. The

---

31. As I wrote earlier:

> The stiffer the penalties, the less likely it is that an individual will commit an offence. Very few people are likely to distribute music or movies without authorization of the copyright holders if they will be sent to jail for thirty years—or worse, if one or both of their hands are to be chopped off.

Peter K. Yu, *Digital Copyright Reform and Legal Transplants in Hong Kong*, 48 U. LOUISVILLE L. REV. (forthcoming 2010), *available at* http://ssrn.com/abstract=1538638 (manuscript at 7).

32. *See* Strowel, *supra* note 2, at 86 ("[T]he simple possibility of banishment from the internet would play this role for most internet users."); Donna St. George, *A New-age Twist on the Age-old Parenting Technique of Grounding*, WASH. POST, at A4, *available at* 2010 WLNR 17771073 (extolling the benefits and effectiveness of digital grounding).

33. Barry Sookman & Daniel Glover, *Why the* Copyright Act *Needs a Graduated Response System*, LAW. WKLY., Jan. 2010, at 10, *available at* http://www.lawyersweekly-digital.com/lawyersweekly/2934?pg=10.

graduated response system also alters the internal calculus users may have in determining whether illegal downloading is worth their effort.[34] In fact, because only a small minority of uploaders supplied the infringing materials for others to download,[35] the system may greatly strengthen the protection for copyright holders by altering the behavior of some active uploaders.

To be certain, there remain some recidivist hardcore uploaders who will actively evade the system by developing or deploying circumvention technologies, providing new email addresses or fraudulent data, using others' personal identifying information or credit cards, or exploiting public Wi-Fi or WiMax networks or their neighbors' open wireless connections. However, the goal of the graduated response system is not to eliminate once and for all massive online copyright infringement—a goal virtually impossible to achieve.[36] Rather, the goal is to reduce leakage to ensure *reasonable and adequate* compensation for the copyright holders' creative endeavors.[37] As the content and user-generated content service industries jointly recognized in the Principles for User Generated Content Services, "no system for deterring infringement is or will be perfect."[38] Moreover, as Professor Alain Strowel wrote recently, "[A] solution that would eliminate all piracy, if at all possible, would seem dangerous or at least dubious for both individual liberties and technological innovation."[39]

Finally, the use of the graduated response system provides an efficient, cost-effective, and streamlined process to combat massive online copyright

34. *See* Olivier Bomsel & Heritiana Ranaivoson, *Decreasing Copyright Enforcement Costs: The Scope of a Graduated Response*, REV. ECON. RES. ON COPYRIGHT ISSUES, Dec. 2009, at 13, 27.

35. *See* Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, FIRST MONDAY (Oct. 2, 2000), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/792/701 (citing a study by researchers at Xerox's Palo Alto Research Center showing that the top 20% of Gnutella users were responsible for 98% of all the files shared).

36. *See* Peter K. Yu, *Anticircumvention and Anti-anticircumvention*, 84 DENV. U. L. REV. 13, 72 (2006) (noting the impossibility of developing a copyright system that has zero leakage); *accord* June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385, 477 (2004) ("*Some* piracy has always been a cost of doing business, but there comes a point at which it is realistic—and unfair—to expect paying customers to subsidize widespread free use."); Alfred C. Yen, *What Federal Gun Control Can Teach Us About the DMCA's Anti-Trafficking Provisions*, 2003 WIS. L. REV. 649, 691 ("[N]o law—not even a complete ban on circumvention technology—can guarantee the security of copyright. Piracy has always existed, yet copyright-based industries have flourished.").

37. *See* Yu, *supra* note 36, at 72. Professor Paul Geller, for example, insightfully distinguished between leakage and hemorrhage. *See* Paul Goldstein, *Summary of Discussion*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 241, 244 (P. Bernt Hugenholtz ed., 1996) (noting Professor Geller's apt distinction "between copyright 'leaks' and copyright 'haemorrhages'").

38. Principles for User Generated Content Services, http://www.ugcprinciples.com/ (last visited Sept. 18, 2010).

39. Strowel, *supra* note 2, at 86.

infringement.[40] It can help rights holders save a great deal of money that has been spent needlessly on civil lawsuits,[41] not to mention the fact that these unpopular lawsuits have threatened to make the recording industry "the most hated industry since the tobacco industry."[42] By building enforcement actions into the network and taking an approach that does not force ISPs to disclose information about their subscribers, the system is also more protective of the users' privacy interests.[43]

Even if the system can function only as a scarecrow, this digital scarecrow will still provide a symbolic reminder that there may be serious consequences to unauthorized reproduction and distribution of copyrighted works.[44] It is small wonder that Olivier Bomsel, a French industrial economics professor, described the graduated response system as "the best long term means to internalize the costs of free-riding while decreasing the costs associated with copyright enforcement."[45]

---

40. As Professor Strowel pointed out:

> The graduated response system shares similar objectives and some characteristics with the UDRP type of mechanism: the speed of the procedure, its effectiveness (implementation by an intermediary, i.e. the registrar or the access provider), the limited cost of the mechanism (in comparison with standard court proceedings), the focus on resolving straightforward infringement cases involving rather basic facts, the possibility of an appeal before a judicial court, etc.

Id. at 78.

41. *See* Greg Sandoval, *A Year Out, Where's RIAA's Promised ISP Help?*, CNET NEWS, Dec. 23, 2009, http://news.cnet.com/8301-31001_3-10420803-261.html.

42. Knopper, *supra* note 4.

43. This claim, however, has been questioned by privacy advocates. *See* discussion *infra* Part I.B.2.

44. As journalist Greg Sandoval reported:

> Multiple music sources have told me over the past month the RIAA leaders were feeling pressure to drop the lawsuit campaign, but were also being lobbied by some at the labels to put some kind of deterrent in place, even if totally toothless. They didn't want the public to think there weren't any consequences to pirating music, even if the reality was exactly that.

Sandoval, *supra* note 41; *accord* COMMERCE & ECON. DEV. BUREAU, H.K. SPECIAL ADMIN. REGION, PRELIMINARY PROPOSALS FOR STRENGTHENING COPYRIGHT PROTECTION IN THE DIGITAL ENVIRONMENT (ANNEX B) 1–2 (2008), *available at* http://www.cedb.gov.hk/citb/ehtml/Consultation_Document_Prelim_Proposals_Eng%20(full).pdf ("[S]ome copyright owners remain adamant that the current civil remedies, though difficult to enforce, should be kept if only as a deterrent.").

45. Olivier Bomsel, *The Costs and Benefits of Graduated Response in Copyright Enforcement*, http://www.barrysookman.com/2010/02/01/the-costs-and-benefits-of-graduated-response-in-copyright-enforcement/ (Feb. 1, 2010); *see also* Bomsel & Ranaivoson, *supra* note 34 (discussing the ability of the graduated response system to significantly reduce enforcement costs and to restore incentives along the copyright distribution chain).

2. ISPs

The graduated response system helps ensure that ISPs can continue to develop and improve their service without worrying about the constant need to respond to lawsuits and the high costs of legal defense.[46] This is particularly important when the providers have deep pockets that greatly increase their vulnerability to lawsuits, making them scapegoats for their users' infringing activities. To some extent, the system serves the same purpose as that of the Internet safe harbor provided by § 512 of the Copyright Act;[47] chapter II, § 4 of the EU E-Commerce Directive;[48] and other similar laws, regulations, and directives.

In addition, the graduated response system acknowledges the fact that ISPs often do not have control over the considerable amount of copyrighted materials stored on their websites or disseminated through their networks. Under most circumstances, ISPs "may merely be innocent third parties playing a passive role when infringing activities occur on their service platform."[49] Nevertheless, the system also recognizes the need to allocate responsibility for protecting copyrighted materials among copyright holders, ISPs, and Internet users. One of the greatest benefits of the graduated response system, indeed, is to facilitate cooperation between copyright holders and ISPs. As Professor Strowel elaborated:

> "Graduated response" . . . refers to an alternative mechanism to fight internet piracy (in particular resulting from P2P file sharing) that relies on a form of co-operation with the internet access providers that goes beyond the classical "notice and take down" approach, and implies an educational notification mechanism for alleged online infringers before more stringent measures can be imposed (including, possibly, the suspension [or] termination of the internet service). The "graduated response" is another word for improved ISP co-operation.[50]

---

46. *See* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1887–88 (2000) ("ISPs also will flourish because they need not fear liability for the acts of their subscribers. This in turn might make Internet access less expensive to future subscribers.").

47. 17 U.S.C. § 512 (2006).

48. Council Directive 2000/31, On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, arts. 12–15, 2000 O.J. (L 178) 1, 12–13; *see also* Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481, 481–94 (2009) (discussing the different approaches taken by the United States in the DMCA and the European Union in the E-Commerce Directive).

49. COMMERCE, INDUS. & TECH., H.K. SPECIAL ADMIN. REGION, COPYRIGHT PROTECTION IN THE DIGITAL ENVIRONMENT at iv (2007).

50. Strowel, *supra* note 2, at 77; *see also* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. (forthcoming 2010),

Moreover, the graduated response system can help ISPs direct traffic and reduce network congestion. To some extent, ISPs are just as concerned and annoyed as the copyright holders over the massive illegal online file-sharing activities. While copyright holders were concerned over their potential lost sales and the growing lack of respect for copyright, ISPs were annoyed by how Internet file-sharers have abused the service by hogging bandwidth, congesting the network, and reducing the overall user experience of most other subscribers.

One may still remember the time when colleges and universities were concerned about the high costs of computing resources that were allocated to music downloads as well as the resulting network congestion that interfered with teaching and research during the height of the Napster boom.[51] As the Indiana University student newspaper lamented at that time, "'Students attempting to hunker down to coursework should not have to be inconvenienced by a strain on the network.'"[52] Eventually, some universities had no choice but to ban Napster from campus networks.[53] The graduated response system, therefore, provides a win-win-win for copyright holders, ISPs, and those users who do not participate in illegal file-sharing activities.

ISPs initially fought hard against the aggressive legal tactics the entertainment industry took, in part to protect the privacy of their customers and in part to ensure greater penetration of their broadband market—both of which relate to the providers' economic bottom line. In recent years, however, their interests seem to have converged with those of the entertainment industry. Today, ISPs seem to have migrated from a model that provides mere "dumb pipes" to one that includes premium

---

available at http://ssrn.com/abstract_id=1565038 (manuscript at 4) (describing the graduated response system as a "division of labor between rights owners and ISPs with respect to monitoring and notification of infringement [that] varies from one permutation of graduated response to the next").

51. *See* Yu, *P2P and the Future*, *supra* note 1, at 702–03. As one commentator explained:

> Napster users eat up large and unbounded amounts of bandwidth. By default, when a Napster client is installed, it configures the host computer to serve MP3s to as many other Napster clients as possible. University users, who tend to have faster connections than most others, are particularly effective servers. In the process, however, they can generate enough traffic to saturate a network. It was this reason that Harvard University cited when deciding to allow Napster, yet limit its bandwidth use.

Roger Dingledine, *Accountability*, *in* PEER-TO-PEER: HARNESSING THE BENEFITS OF A DISRUPTIVE TECHNOLOGY 271, 271 (Andy Oram ed., 2001).

52. JOHN ALDERMAN, SONIC BOOM: NAPSTER, MP3, AND THE NEW PIONEERS OF MUSIC 112 (2001) (external citation omitted).

53. Ellie Kieskowski, *Napster Banned at 40 Percent of Colleges and Universities*, STREAMINGMEDIA.COM, Aug. 30, 2000, http://www.streamingmedia.com/Articles/News/Featured-News/Napster-Banned-at-40-Percent-of-Colleges-and-Universities-63035.aspx.

entertainment content. As RIAA President Cary Sherman acknowledged in a recent interview concerning the graduated response system:

> There was a time five years ago when ISPs were solely focused on increasing their broadband penetration, and cutting back on piracy was not part of their business interest. Five years later, they're in a very different place. They want to be portals in their own right, they want to offer their subscribers great content; it's something that distinguishes one from another. They're looking at themselves as more than the dumb pipes that they were five years ago, and I think that opens up partnerships that didn't exist before.[54]

Consider Comcast, for example. In December 2009, it struck a deal with General Electric to acquire a majority stake in NBC Universal.[55] Less than a year later, Comcast reached a ten-year licensing agreement with CBS, including provisions that would allow its subscribers to watch CBS content online.[56]

Furthermore, while ISPs still have a strong interest in increasing their market share, their economic bottom line, along with the high resource and administrative costs and the concerns over network congestion, may eventually force them to take action to boot some illegal file-sharers off their network. As David Nimmer, the author of the leading copyright treatise, explained:

> Presumably, every time a notification of claimed infringement is served as to subscriber *F*, the provider incurs a charge to take down the subject material and provide appropriate notifications. If *F* replies with his own counter-notification, additional expenses presumably accrue as to put-back. Accordingly, even if *F* pays $50/month for the privilege of being a subscriber, at a certain point the provider will be forced to consider him a money-losing proposition. It would likely then choose to exercise its contractual rights of pulling the plug on him. The only point here is that Congress did not command that providers must determine in advance where that point will be reached, through mandating its inclusion in a repeat infringers policy.[57]

---

54. Anderson, *supra* note 4. Similarly, one analyst noted: "One reason for that may be that many bandwidth providers want greater access to top entertainment content. The best example of that is Comcast's proposed acquisition of NBC Universal. To many in the film and music sectors, it appears that the interests of entertainment companies and ISPs are aligning." Sandoval, *supra* note 41.

55. Tim Arango, *G.E. Makes It Official: NBC Will Go to Comcast*, N.Y. TIMES, Dec. 4, 2009, at B3, *available at* http://www.nytimes.com/2009/12/04/business/media/04nbc.html.

56. Brian Stelter, *CBS and Comcast Reach a 10-Year Deal on Fees*, N.Y. TIMES, Aug. 3, 2010, at B5.

57. 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.10[B][3][b]

In the future, if ISPs undertake deep packet inspection and monitoring to direct traffic, differentiate pricing, promote quality of service (QOS), or all or some of the above,[58] their positions may converge even further with those of the copyright holders. After all, the more an ISP wants to discriminate Internet traffic, the more it has to evaluate the transmitted content to prioritize traffic, and the more knowledge it will acquire that, in turn, makes it difficult for the ISP to claim safe harbor protection under § 512 of the Copyright Act. As Professor Rob Frieden explained:

> While [such] monitoring by itself may not eliminate the safe harbor qualification, deep packet monitoring probably does because the packet header information likely will identify significant information about the nature and type of traffic sufficient to put the ISP on actual notice of any copyright infringement. While the ISP needs only information about QOS and other features for which a particular user and user generated traffic stream qualifies, the ISPs cannot lawfully ignore copyright status if such information becomes part of the standard header information ISPs routinely inspect and process.
>
> . . . .
>
> Given the risk of losing a safe harbor, ISPs likely will err on the side of accommodating DRM [digital rights management] cooperation requests from copyright holders. ISPs probably will collaborate with copyright holders, perhaps going so far as to program hardware with deep packet inspection software that achieve both traffic management goals, to pursue price and QOS diversification, as well as DRM, to mollify copyright holders.[59]

3. Internet Users

The graduated response system provides an attractive alternative to the highly unpopular lawsuits the entertainment industry thus far has filed

---

(rev. ed. 2010); *see also* Frieden, *supra* note 11, at 637 ("The decision to engage in active management of content results not from an affirmative obligation to do so, but instead the desire to tap new business opportunities accruing from the ability to scrutinize bitstreams.").

58. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1426 (discussing the different motives and pressures that push toward greater ISP surveillance).

59. Frieden, *supra* note 11, at 656, 674. Similarly, Professor Bridy observed:

> As broadband business models evolve away from the traditional model of passive carriage, ISPs risk sacrificing the special protections that have developed over time to shield neutral intermediaries from liability for copyright infringement. This potential exposure gives ISPs a compelling incentive to explore private partnerships with rights owners that would once have been politically unthinkable.

Bridy, *supra* note 50 (manuscript at 4).

against more than 35,000 individual file-sharers.[60] Since the initiation of these lawsuits in 2003, the industry has been heavily criticized for its strong-arm tactics.[61] Although the RIAA has already announced its plan to cease using those tactics against individual file-sharers, it remains unclear whether the industry will actually abandon those tactics or whether it will only scale back some of its prior efforts to alleviate the public outcry.[62]

As William Patry pointed out, notwithstanding its widely publicized announcement, "the RIAA has indicated that it will continue to sue those who in its opinion are engaged in substantial downloading, that it will continue to prosecute suits already filed, and that it will file future suits that are in the 'pipeline.'"[63] Reports have also shown that the industry has filed lawsuits as late as December 15, 2008, even though the industry made the announcement that month and claimed publicly that it had not filed lawsuits against individuals for months.[64] The graduated response system also helps alleviate some of the public concern over the lack of proportionality between the award of heavy statutory damages in some recent high-profile cases[65] and the highly questionable, and often hard-to-prove, harm caused by individual file-sharing activities.[66] For example, in

60. von Lohmann, *supra* note 30.

61. For criticisms and analysis of these strong-arm tactics, see generally Peter K. Yu, *The Copyright Divide*, 25 CARDOZO L. REV. 331, 387–401 (2003); Yu, *The Escalating Copyright Wars*, *supra* note 1, at 910–23; Yu, *P2P and the Future*, *supra* note 1, at 658–98.

62. *See* PATRY, *supra* note 17, at 11.

63. *Id*.

64. *See, e.g.*, David Kravets, *RIAA Qualifies Statement on No New Copyright Lawsuits*, WIRED, Dec. 23, 2008, http://www.wired.com/threatlevel/2008/12/riaa-qualifies/; Mike Masnick, *RIAA Caught Lying About Stopping Lawsuits*, TECHDIRT, Dec. 21, 2008, http://www.techdirt.com/articles/20081221/1519113180.shtml. The difference could perhaps be explained by the imprecise nature of the public announcement and by the fact that those lawsuits were already in the "pipeline."

65. *See* Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 441 (2009) ("Awards of statutory damages are frequently arbitrary, inconsistent, unprincipled, and sometimes grossly excessive."); J. Cam Barker, Note, *Grossly Excessive Penalties in the Battle Against Illegal File-Sharing: The Troubling Effects of Aggregating Minimum Statutory Damages for Copyright Infringement*, 83 TEX. L. REV. 525 (2004) (criticizing statutory damages in the context of online file-sharing activities).

66. As I wrote earlier:

> [U]nauthorized reproduction and distribution do not always result in financial harm to the copyright holder. Many file sharers are simply not interested in buying the products or are unable to afford them. At times, the potential infringing activities may also benefit copyright holders. For example, after sampling a song or a portion of the movie online, some downloaders may decide to purchase the album or the DVD. Even if they do not purchase the product they have already listened to or viewed, they may purchase future works created by the same artist or producer. Without sampling, many downloaders are unlikely to be aware of the products or be interested in making purchase in the first place.

Capitol Records, Inc. v. Thomas, a Minnesota woman was fined more than $1.92 million for the infringement of "24 songs—the equivalent of approximately three CDs, costing less than $54."[67] This damage award, which was calculated following a new trial, more than octupled the original damage award of "$222,000—more than *five hundred* times the cost of buying 24 separate CDs and more than *four thousand* times the cost of three CDs."[68] Likewise, a graduate student from Boston University was fined $675,000 for providing copyrighted works without the authorization of the copyright holders.[69] Courts have since drastically reduced both of these awards—the former by 97% and the latter by 90%.[70]

In addition, the graduated response system may help direct prosecutors' energies and resources to more serious online file-trafficking activities, as opposed to the garden-variety file sharing by individual Internet users. In November 2005, in a highly controversial criminal trial in Hong Kong, an individual was sentenced to three months in jail for uploading *Daredevil*, *Miss Congeniality*, and *Red Planet* using BitTorrent technology.[71] Although the widely-publicized jail term successfully intimidated individual file-sharers for a short period of time, this case had limited long-term effects. Compared to, say, the eighteen-month jail term handed out in the recent criminal trial of "a high-level member of an Internet piracy organization known as 'Elite Torrents'"—the first criminal action in the United States against peer-to-peer file-sharers[72]—the verdict in Hong Kong seems rather unfair and overreactive.

In short, the graduated response system provides an attractive alternative to many of the unpopular legal tactics employed in civil lawsuits and criminal prosecutions. To be certain, the system is still not as attractive as a plea bargain in which the individual infringer can bargain down his or her penalty from a jail term or a heavy fine to Internet

---

Yu, *supra* note 31 (manuscript at 10–11).

67. 579 F. Supp. 2d 1210, 1227 (D. Minn. 2008).

68. *Id*. (emphasis in original modified).

69. Editorial, *Awkward Download Laws Make Music-sharing Case a Travesty*, BOSTON GLOBE, Dec. 14, 2009, § Editorial Opinion, at 18.

70. *See* Nate Anderson, *Judge Slashes "Monstrous" P2P Award by 97% to $54,000*, ARS TECHNICA, Jan. 22, 2010, http://arstechnica.com/tech-policy/news/2010/01/judge-slashes-monstrous-jammie-thomas-p2p-award-by-35x.ars; Rosie Swash, *Filesharer Joel Tenenbaum Has Fine Reduced by 90%*, GUARDIAN (London), July 12, 2010, http://www.guardian.co.uk/music/2010/jul/12/filesharer-joel-tenenbaum.

71. Chan Nai Ming v HKSAR, [2007] 10 H.K.C.F.A.R. 273 (C.F.A.), http://legalref.judiciary.gov.hk/lrs/common/ju/judgment.jsp.

72. United States v. Dove, 585 F. Supp. 2d 865, 867 (W.D. Va. 2008). The perpetrator eventually "was sentenced to 18 months in prison . . . for his role in the organization." Sam Wood, *Ex-Drexel Student Gets Probation in Internet Piracy*, PHILA. INQUIRER, Sept. 17, 2008, at B4, *available at* http://www.allbusiness.com/crime-law/criminal-offenses-cybercrime/12145752-1.html; *see also Feds Foil 'Sith' Site*, ST. PAUL PIONEER PRESS (Minn.), May 26, 2005, at C2, *available at* 2005 WLNR 22959975 (noting first U.S. criminal case against torrent downloaders).

disconnection. The system is also rather different from a choice between the usual four-figure monetary settlement and Internet disconnection, though it admittedly is an improvement over what Professor Lawrence Lessig described as "a mafia-like choice" between a costly settlement and an outrageously high legal bill incurred in defending the lawsuit.[73]

Nevertheless, the graduated response system is still much better than one that overly criminalizes a large number of Internet users, many of whom may be future pillars of our society. As Professor Lessig lamented in his most recent book, *Remix*:

> I worry about the effect this [copyright] war is having upon our kids. What is this war doing to them? Whom is it making them? How is it changing how they think about normal, right-thinking behavior? What does it mean to a society when a whole generation is raised as criminals?[74]

In fact, if the trend of criminalization continues, its social impact is likely to be rather significant, and the costs of programs that are needed to rehabilitate "copyright criminals" will only increase. Even worse, "taxpayers will have to bear the high costs of enforcement and rehabilitation, while there is no guarantee that criminalization would induce the creation of more socially beneficial works or that citizens could be more law-abiding outside the copyright world."[75]

B. *Drawbacks*

While the benefits of the graduated response system are significant, there are also rather serious drawbacks. Although the graduated response system includes such draconian sanctions as Internet disconnection,[76] it also covers other less draconian alternatives, such as bandwidth reduction, monitored access, and site, port, or protocol blocking. Nevertheless, the discussion in this Article focuses primarily on Internet disconnection, for three reasons.

First, the suspension of Internet access for a fixed period of time is a key measure incorporated into the graduated response system to provide deterrent effect. Because Internet disconnection is generally considered the endgame of the graduated response system, it is logical for this Article to focus on this particular sanction if we are to provide an accurate, candid,

---

73. LAWRENCE LESSIG, FREE CULTURE 51–52 (2004); *see also* Yu, *supra* note 31 (manuscript at 18).

74. LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY xvii (2008).

75. Yu, *supra* note 31 (manuscript at 9).

76. *See* Strowel, *supra* note 2, at 85 ("[T]he graduated response is not just about its terminal phase—the termination of internet accounts. It also relies on an automatic warning system, and we can expect that the warning system will deter some potential infringers.").

and complete assessment of the system. Second, Internet disconnection has serious implications beyond the protection of intellectual property rights. The discussion of Internet disconnection therefore will help underscore the system's many major shortcomings both within and without the intellectual property arena. Third, in an effort to provide some recommended principles on how to develop an acceptable graduated response system, as Part IV will outline, this Part closely examines the most draconian sanction. After all, if the proposed principles work for Internet disconnection, they are likely to work for other less draconian sanctions as well.

1. ISPs

To begin with, the benefits to ISPs discussed above are likely to be quickly outweighed by the system's attendant costs and unintended side effects. The graduated response system can be rather costly to ISPs in two ways. First, the system would substantially raise the costs of surveillance, policing, and data retention that ISPs are to undertake. As Professor Michael Geist recounted:

> Initial [estimates by the UK government] peg the expense to Internet providers alone at as much as 500 million pounds . . . over ten years. This includes the costs of identifying subscribers, notifying them of alleged infringements, running call centres to answer questions, and investing in new equipment to manage the system. As a result, the UK government estimates that 40,000 people could lose Internet access due to anticipated increases in subscriber fees.[77]

Even more problematic, such costs vary significantly depending on the size of the ISP. As Professor Geist continued, the 2006 Industry Canada commissioned study has shown that "the cost of a single notification was $11.73 for larger Internet providers (more than 100,000 subscribers) and $32.73 for smaller Internet providers."[78]

To be certain, ISPs should assume some responsibility for protecting copyrighted materials, especially when they have obtained considerable, and often direct, financial benefits from Internet users.[79] The need for these

77. Michael Geist, *Estimating the Cost of a Three-Strikes and You're Out System*, TORONTO STAR, Jan. 26, 2010, http://www.thestar.com/business/article/755443--geist-three-strikes-and-you-re-out-system-draw-cries-of-foul-from-governments. Those costs will be greatly reduced if the graduated system is designed as a fully automated system—perhaps with the help of deep packet inspection or other networking management tools.

78. *Id*.; *see also* Greg Sandoval, *One ISP Says RIAA Must Pay for Piracy Protection*, CNET NEWS, Dec. 22, 2008, http://news.cnet.com/8301-1023_3-10127841-93.html (discussing the challenge confronting small ISPs).

79. *Cf*. Strowel, *supra* note 2, at 86 ("Things will only change if the access providers

users to share and use content freely without the copyright holders' authorization, undoubtedly, has increased their demand for high-end services and bandwidths. At some point, however, that financial burden may become just too great for ISPs to shoulder. Such burden, in turn, would also make it difficult for ISPs to improve their network, to continue to offer low-cost services for users, or both. Indeed, the concerns over these financial burdens and the societal interest in a greater rollout of Internet services were the primary justifications for establishing the ISP safe harbor in the first place.[80]

Even worse, the graduated response system would put ISPs in a catch-22 situation in which the providers would be confronted with a Hobson's choice of high investigation costs and significantly reduced experience. If ISPs were to fully investigate the potential infringing activities, the costs of such investigation could be prohibitive. They might also lose the safe harbor protection the current law extends to them. However, if they failed to undertake a full investigation and merely relied on the copyright holders' accusations, the user experience could be significantly reduced. In turn, such reduced user experience, along with decreased privacy protection, would translate into unhappy or lost customers as well as reduced profits for ISPs. Either way, the graduated response system would significantly harm ISPs.[81]

While most ISPs are likely to err on the side of copyright holders, some ISPs may choose to err on the side of Internet users. Some may even use their resistance to takedown notices or their refusal to turn over subscribers as a consumer choice point to attract business. Notwithstanding these initiatives, "the lack of public discussion of [these choice points may] suggest[] that consumers have little awareness of the issue or means to compare [ISP] behavior on this issue."[82] Given the industry's aggressive

---

themselves become more active in policing their clients because they see and reap some benefits.").

80. *See* S. REP. NO. 105-190, at 1–2 (1998) (stating that the DMCA was "designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age"); David Nimmer, *Repeat Infringers*, 52 J. COPYRIGHT SOC'Y U.S.A. 167, 169 (2005) ("Section 512 promotes Internet commerce and online speech by setting forth various safe harbors.").

81. Professor Bridy recently made a similar point:

> The provider finds itself caught between Scylla and Charybdis: if it fails to terminate a user's access after receiving repeat notices of infringement from a copyright owner, it faces the loss of the safe harbor for not having reasonably implemented its termination policy; if, on the other hand, it terminates a user's access on the copyright owner's say-so, it faces the loss of a customer, which is especially troubling if the claims of infringement turnout to be misdirected or non-meritorious. Moreover, wrongful terminations might themselves create the potential for provider liability to customers for breach of contract.

Bridy, *supra* note 50 (manuscript at 17).

82. Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER &

legal tactics and the ISPs' increasing reluctance to openly challenge the industry's position, any evidence about such potential choice points is likely to be anecdotal, if it exists at all.

It is therefore no surprise that commentators have increasingly advocated the ISP's duty to fully disclose their policy to subscribers. As Professor Strowel reminded us:

> [T]he measure of internet suspension will appear more justified as a means of protecting the right of third parties if the contract with the access provider adequately defines the circumstances under which access can be blocked, and specifies repeat infringements can lead to the extreme measure of internet access restriction.[83]

After Comcast's recent fiasco over its throttling of Internet traffic involving BitTorrent users,[84] the FCC has begun to explore greater regulation of network management. As the FCC declared:

> We . . . note that because "consumers are entitled to access the *lawful* Internet content of their choice," providers, consistent with federal policy, may block transmissions of illegal content (*e.g.*, child pornography) or transmissions that violate copyright law. To the extent, however, that providers choose to utilize practices that are not application or content neutral, the risk to the open nature of the Internet is particularly acute and the danger of network management practices being used to further anticompetitive ends is strong.[85]

In November 2009, the FCC issued a notice for proposed rulemaking that underscored the need to subject broadband providers to "reasonable network management,"[86] which is further defined to include:

HIGH TECH. L.J. 621, 687 (2006).

83. Strowel, *supra* note 2, at 84; *see also* Bridy, *supra* note 50 (manuscript at 53) ("Broadband providers should provide full disclosure of their copyright enforcement practices to prospective and existing customers, including whether they use packet inspection or other intrusive technology for copyright enforcement purposes.").

84. *See In re* Formal Complaint of Free Press and Public Knowledge, 23 F.C.C.R. 13,028, 13,028 (2008), *order vacated sub nom.* Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010). For discussions of Comcast's controversial attempts to throttle internet traffic involving the BitTorrent peer-to-peer protocol, see generally Christopher S. Yoo, *Network Neutrality After Comcast: Toward a Case-by-Case Approach to Reasonable Network Management*, *in* NEW DIRECTIONS IN COMMUNICATIONS POLICY 55 (Randolph J. May ed., 2009); Ohm, *supra* note 58, at 1435–36; Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529, 565–69 (2009).

85. *In re Formal Complaint of Free Press and Public Knowledge*, 23 F.C.C.R. at 13,058.

86. Preserving the Open Internet, Broadband Industry Practices, 74 Fed. Reg. 62,638, 62,638 (proposed Nov. 30, 2009). As the notice for proposed rulemaking stated:

> (a) Reasonable practices employed by a provider of broadband Internet access service to (i) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; (ii) address traffic that is unwanted by users or harmful; (iii) prevent the transfer of unlawful content; or (iv) prevent the unlawful transfer of content; and (b) other reasonable network management practices.[87]

2. Internet Users

The biggest drawbacks of the graduated response system impact Internet users. First, the system denies end-users due process by subjecting them to unverified suspicion of infringing activities. As William Patry explained:

> Notices of alleged infringement are not, as popularly assumed, the result of copyright owners sitting down at a computer terminal and *directly* detecting infringement. Instead, notices of alleged infringement are generated automatically by the millions, by third-party companies hired by copyright owners. This process, which involves *indirect* detection of alleged unauthorized activity, relies on automated webcrawler technology and databases of digital fingerprints. The process has been notoriously inaccurate, leading to lawsuits against people who don't even have computers or who are dead, as well as takedown notices sent to individuals claiming that wholly original videos created by those individuals are infringing.

> Specifically, we propose that all providers of broadband Internet access service must comply with the following four rules:
>
> 1. Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from sending or receiving the lawful content of the user's choice over the Internet.
>
> 2. Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from running the lawful applications or using the lawful services of the user's choice.
>
> 3. Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from connecting to and using on its network the user's choice of lawful devices that do not harm the network.
>
> 4. Subject to reasonable network management, a provider of broadband Internet access service may not deprive any of its users of the user's entitlement to competition among network providers, application providers, service providers, and content providers.

Id. at 62,645; *see also* Bridy, *supra* note 50 (manuscript at 2) (discussing this notice for proposed rulemaking).

87. Preserving the Open Internet, Broadband Industry Practices, 74 Fed. Reg. at 62,650.

> Faced with the receipt of hundreds of thousands or millions of such notices under graduated response, ISPs will simply pass the notices along to customers, who will be presumed guilty. Unlike court proceedings, where consumers are presumed innocent, and are afforded due process of law and defenses such as fair use, under private enforcement by ISPs on copyright owner's behalf, there is no guarantee or even reason to believe ISPs' customers will be able to get service restored due to errors or that they will have the ability to prove their use was lawful as fair use.[88]

To make matters worse, the infringement-identifying technology has been fairly unreliable thus far. Since the recording industry began sending out cease and desist letters a few years ago, there have been reports of some highly disturbing cases of misidentification. Consider the following examples. The industry's web-crawlers confused an a cappella song about a gamma ray satellite developed by Pennsylvania State University with the heavily downloaded songs of a best-selling rhythm-and-blues artist.[89] The RIAA sent a notice to a national broadband provider alleging that one of its subscriber sites had illegally "offer[ed] approximately 0 sound files for download."[90] Warner Brothers misidentified a child's book report on *Harry Potter and the Sorcerer's Stone* as an infringing Harry Potter movie, even though the file was only of one kilobyte and in rich text format.[91] A 66-year-old Boston woman was accused of offering hardcore rap songs, like "I'm a Thug," for download, even though her computer was incapable of running the file-swapping software she allegedly had used.[92] A sick

---

88. PATRY, *supra* note 17, at 13.

89. *Complaint from Recording Industry Almost Closes Down a Penn State Astronomy Server*, CHRON. HIGHER EDUC. (Wash., D.C.), May 23, 2003, http://chronicle.com/article/complaint-from-recording-in/28802/.

90. Declan McCullagh, *RIAA Apologizes for Erroneous Letters*, CNET NEWS, May 13, 2003, http://news.com.com/2100-1025-1001319.html (internal quotation marks omitted).

91. Symposium, *Copyright & Privacy—Through the Copyright Lens*, 4 J. MARSHALL REV. INTEL. PROP. L. 212, 219 (2005) (remarks of Sarah B. Deutsch, vice president & associate general counsel for Verizon Communications Inc.).

92. As the *Boston Globe* reported:

> Among the songs she was accused of sharing: "I'm a Thug," by the rapper Trick Daddy.
>
> But Ward, 66, is a "computer neophyte" who never installed file-sharing software, let alone downloaded hard-core rap about baggy jeans and gold teeth, according to letters sent to the recording industry's agents by her lawyer, Jeffrey Beeler.
>
> Other defendants have blamed their children for using file-sharing software, but Ward has no children living with her, Beeler said.
>
> Moreover, Ward uses a Macintosh computer at home. Kazaa runs only on Windows-based personal computers.

Chris Gaither, *Recording Industry Withdraws Suit*, BOSTON GLOBE, Sept. 24, 2003, at C1, *available at* 2003 WLNR 3414336; *see also* John Schwartz, *She Says She's No Music Pirate. No Snoop Fan*,

teenager was sued for sharing ten songs via peer-to-peer networks when she was in hospital receiving weekly treatments for pancreatitis.[93] And the most troubling of all, the RIAA filed a lawsuit against an eighty-three-year-old deceased woman who hated computers during her lifetime, causing one newspaper reporter to write: "Death is no obstacle to feeling the long arm of the Recording Industry Ass. of America."[94]

If these examples are not enough, the industry has been rather unapologetic toward the misidentified victims. As Cory Doctorow pointed out, in response to the misidentification cases, Dan Glickman, the chairman and CEO of the Motion Picture Association of America, reportedly has said, "When you go trawling with a net, you catch a few dolphins."[95] His unapologetic attitude (and that of others) no doubt has exacerbated the concerns civil liberties groups, consumer advocates, and academic commentators already have.

In the past few years, identification, fingerprinting, and watermarking technologies have greatly improved. As Cary Sherman pointed out, the

---

Either, N.Y. TIMES, Sept. 25, 2003, at C1.

93. Steve Ragan, *RIAA Sues Hospitalized Girl—Court Issues Default Judgment*, TECH. HERALD, Dec. 9 2008, http://www.thetechherald.com/article.php/200850/2592/RIAA-sues-hospitalized-girl-court-issues-default-judgment.

94. Andrew Orlowski, *RIAA Sues the Dead*, THE REGISTER, Feb. 5, 2005, http://www.theregister.co.uk/2005/02/05/riaa_sues_the_dead/.

95. Cory Doctorow, *Online Censorship Hurts Us All*, GUARDIAN (London), Oct. 2, 2007, http://www.guardian.co.uk/technology/2007/oct/02/censorship (internal quotation marks omitted). While Glickman's reported remark points to the inevitability of false positives, it does not justify such action. The Marine Mammal Protection Act of 1972, for example, was enacted to protect dolphins from being killed needlessly by those catching yellowfin tuna. Marine Mammal Protection Act of 1972, Pub. L. No. 92-522, 86 Stat. 1027, 1041 (codified as amended at 16 U.S.C. §§ 1361–1407 (2006)). Likewise, dolphin-safe labels have been used to encourage consumers to purchase canned tuna that have been caught without maiming or killing dolphins. *See* Philip Shabecoff, *3 Companies to Stop Selling Tuna Netted with Dolphins*, N.Y. TIMES, Apr. 13, 1990, at A1, *available at* 1990 WLNR 2967700. Interestingly, the entertainment industry's ill-advised overfishing approach has led the Electronic Frontier Foundation and other nonprofit organizations to demand the establishment of an informal "dolphin hotline." As declared in the Fair Use Principles for User Generated Video Content:

> Informal "Dolphin Hotline": Every system makes mistakes, and when fair use "dolphins" are caught in a net intended for infringing "tuna," an escape mechanism must be available to them. Accordingly, content owners should create a mechanism by which the user who posted the allegedly infringing content can easily and informally request reconsideration of the content owner's decision to issue a DMCA takedown notice and explain why the user believes the takedown was improper.
>
> This "dolphin hotline" should include a website that provides information about how to request reconsideration, and a dedicated email address to which requests for reconsideration can be sent. Service providers should ensure that users are informed of these mechanisms for reconsideration . . . .

Fair Use Principles for User Generated Video Content, http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen (last visited Oct. 4, 2010).

latest technology that was recommended for use in the graduated response system had been "examined by a group of engineers at the University of Washington . . . [and was determined to be] the best out there in terms of [the industry's identification] approach."[96] Companies like Audible Magic, which counts among its customers a large number of colleges and universities,[97] also actively promote their services. Audible Magic, in particular, markets its system as "the only graduated response approach with the potential to change file sharers [sic] behaviors and channel them to the ISP's own legitimate content services."[98]

Despite these improvements, it remains troubling that "[r]ecord and motion picture companies have outsourced take-down notices to third-party firms, who rely on automated processes, indirect evidence of infringement, but who have a direct financial incentive to send out as many notices as possible."[99] Given this direct financial benefit, and the outsourced agents' powerful motivation to find as many infringers as they can, it is hard not to question the eagerness of these firms to protect the interests of Internet users.

To some extent, the perverse incentives created by this outsourcing arrangement are similar to those perverse incentives provided to telemarketers who call—or, some would say, harass—individuals to apply for credit cards. Because these telemarketers get paid by the number of credit card applications, they have very limited incentive in either protecting the interests of potential applicants or ensuring that the applicants will continue to keep the card after completing the application. In fact, it would not be a surprise if the applicants were told that they could cancel their card immediately after the application, although they likely would have to call a different number to cancel it!

Second, the graduated response system may undermine the protection of basic human rights and individual liberties.[100] Article 19 of the Universal Declaration of Human Rights provides: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information

96. Anderson, *supra* note 4 (quoting Cary Sherman, president of the RIAA).

97. *See, e.g.*, Audible Magic, CopySense Appliance Customers, http://www.audiblemagic.com/clients-partners/copysense.asp (last visited Oct. 4, 2010).

98. Audible Magic, In-Network Graduated Response, http://audiblemagic.com/pdf/In-Network%20Graduated%20Response.pdf (last visited Oct. 4, 2010).

99. PATRY, *supra* note 17, at 169.

100. *See* HKSAR LEGCO PROPOSALS, *supra* note 19, at 5 ("The 'graduated response' system is clouded by debates over its implications on civil rights and liberties even in jurisdictions where legislation introducing the system has been passed."); *see also* Nimmer, *supra* note 80, at 205 ("First Amendment problems may arise if the repeat infringers limitation is read to permanently bar given individuals from accessing the Internet entirely—particularly as technology evolves and lifeline telephone service is bundled in a given locality with Internet access.").

and ideas through any media and regardless of frontiers."[101] In the digital age, access to the Internet is paramount to the exercise and enjoyment of this core human right. As the district court recognized in *Reno v. ACLU*, the Internet is "the most participatory form of mass speech yet developed,"[102] and the content on this medium "is as diverse as human thought."[103]

To be certain, one could argue that the graduated response system involves mostly private censorship, as opposed to state censorship. As a result, there is no state action and, therefore, no First Amendment violation. While commentators have widely debated whether enforcement of copyright law could constitute state action,[104] the First Amendment claim is likely to be greatly weakened if the system is introduced through private agreements between ISPs and copyright holders. Nevertheless, the free speech concerns described in this Article are those that are inherent in an individual's human rights; they are, therefore, not contingent on the positive interpretation of the First Amendment. There is no doubt that the graduated response system would raise equally serious free speech concerns in countries whose constitutions do not include an equivalent to the First Amendment.

One may further point out that the possibilities for users to obtain alternative online access have greatly mitigated the free speech concerns.[105]

---

101. Universal Declaration of Human Rights art. 19, G.A. Res. 217A, at 71, U.N. GAOR, 3d Sess., 1st plen. Mtg., U.N. Doc. A/810 (Dec. 12, 1948).

102. Reno v. ACLU, 929 F. Supp. 824, 883 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

103. *Id*. at 842; *see also* 47 U.S.C. § 230(a)(3) ("The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."); Jessica Litman, *Sharing and Stealing*, 27 HASTINGS COMM. & ENT. L.J. 1, 50 (2004) (stating that "the idiosyncratic interests of large numbers of individuals who want to share is directly responsible for the wealth and incredible variety of information we can find when we go looking for it").

104. *See* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1607 n.400 (1993) ("Enforcement of property rights should be acknowledged as state action."); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 185 n.179 (1998) ("There's no doubt that a court's enforcement of copyright law to restrict private speech constitutes state action."); Jennifer E. Rothman, *Liberating Copyright: Thinking Beyond Free Speech*, 95 CORNELL L. REV. 463, 508 (2010) ("Under such an understanding, the private enforcement of copyright laws constitutes state action because the laws are authorized by the U.S. Constitution and passed by Congress. . . . Even though the First Amendment has had little success as a defense in copyright cases, no court has suggested that the First Amendment does not apply because there is a state action problem."); Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535, 538 (2004) ("[I]f the First Amendment bars only government action, then copyright law itself ought to be unconstitutional as a government restriction on some speakers in order to improve the relative position of others."). For an excellent discussion of state action, see generally Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503 (1985).

105. *See* Strowel, *supra* note 2, at 83 (noting that an individual user will still "be able to use

Courts, indeed, have severely curtailed the Internet access of convicted criminals.[106] It is important, however, to note the difference between the graduated response system and penalties handed out to criminal convicts. The *alleged* infringing activities that trigger the graduated response system have *yet to be proven* in a court of law, and few of those subject to Internet disconnection are likely to have been convicted criminals. Even if an appeal process were to be built into the system, it remains unclear how one could prove the lack of infringing activities on the Internet or whether a *private* appeal process could be as fair as its *public* counterpart.

Third, and related to the first two, the graduated response system may raise serious concerns over what is generally considered substantive due process under U.S. constitutional law. In a recent article, Professor Jennifer Rothman advanced an affirmative theory to explain why individuals should be able to use another's copyrighted work.[107] She declared:

> Copyright law should be limited when it interferes with the sacred space constitutionally reserved for individuals to define and construct themselves . . . . In [instances where uses of copyrighted works implicate liberty rights in heightened ways], an individual user's liberty interest will most often outweigh countervailing public-policy justifications for protecting copyrighted works as well as the interests of individual copyright holders and creators. Copyrighted works are fundamental to an individual's liberty when their use is integral to the construction of a person's identity. In particular, uses that are necessary for mental integrity, communication, the development and sustenance of emotionally intimate relations, or the practice of one's religion are all at the core of one's identity.[108]

The insights gleaned from her article are important because First Amendment scholars have yet to persuade courts that "individual speech rights should outweigh the speech-producing value of the overall copyright

---

other access points, whether at work, in internet coffee shops, through relatives, or by using devices other than a home computer such as mobile devices with email and browsing capabilities").

106. For discussions of how courts have restricted the internet access of convicted criminals, see generally Emily Brant, Comment, *Sentencing "Cybersex Offenders": Individual Offenders Require Individualized Conditions When Courts Restrict Their Computer Use and Internet Access*, 58 CATH. U. L. REV. 779 (2009); Jessica Habib, Note, *Cyber Crime and Punishment: Filtering Out Internet Felons*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1051 (2004); Doug Hyne, Note, *Examining the Legal Challenges to the Restriction of Computer Access as a Term of Probation or Supervised Release*, 28 N.E. J. ON CRIM. & CIV. CONFINEMENT 215 (2002); Jane Adele Regina, Comment, *ACCESS DENIED: Imposing Statutory Penalties on Sex Offenders Who Violate Restricted Internet Access as a Condition of Probation*, 4 SETON HALL CIRCUIT REV. 187 (2007).

107. Rothman, *supra* note 104.

108. *Id*. at 513.

system."[109] As Justice Ruth Bader Ginsburg declared in *Eldred v. Ashcroft*,[110] "[T]he First Amendment securely protects the freedom to make—or decline to make—one's own speech; it bears less heavily when speakers assert the right to make other people's speeches."[111]

Fourth, the graduated response system may not be effective in inducing a significant change of social behavior among individual file sharers, unless it intends to disconnect a large number of users. As William Patry reminded us: "Graduated response is all stick and no carrot; as such, it can never accomplish its purported goal of encouraging lawful behavior because the industry refuses to respond to the consumer demand, and instead insists on suppressing it, even when third party ISPs are willing to do all the work."[112] Likewise, the Department for Business, Innovation and Skills of the British government declared in its recent *Consultation on Legislation to Address Illicit Peer (P2P) File-Sharing*:

> There is little point in trying to shift consumer behaviour from the unlawful to the legal if there is no legal source which will allow consumers to access the type of content they want in a form and manner that best suits them and at a price they are willing to pay.[113]

To some extent, the system reflects the entertainment industry's ongoing ostrich attitude toward copyright challenges created by the Internet and digital communications technologies. By now, most commentators, and a growing number of industry insiders, have concluded that the industry's business model is somewhat outdated under the current digital environment.[114] Instead of updating the industry's business model to respond to these rapidly-changing conditions, the graduated response system merely perpetuates the outdated thinking that strong-arm tactics would eventually restore profitability to the industry.

Indeed, it is frustrating to notice the belligerent origin of the "graduated response" approach—which dates back to the Kennedy administration and the NATO's response to the Soviet build-up of nuclear missiles—not to mention the disastrous results that escalated responses had brought about during the Vietnam War.[115] Given the persistent confrontational attitude,

---

109. *Id*. at 469.

110. 537 U.S. 186 (2003).

111. *Id*. at 221.

112. PATRY, *supra* note 17, at 12.

113. DEP'T FOR BUS., INNOVATION & SKILLS (U.K.), CONSULTATION ON LEGISLATION TO ADDRESS ILLICIT PEER (P2P) FILE-SHARING 12 (2009).

114. *See, e.g.*, PATRY, *supra* note 17, at 26–30; Yu, *P2P and the Future*, *supra* note 1, at 746–50.

115. *See generally* LAWRENCE FREEDMAN, KENNEDY'S WARS: BERLIN, CUBA, LAOS, AND VIETNAM (2002) (discussing the strategies to steadily increase military action against North

one has to wonder whether the entertainment industry, in fact, has learned anything in the past five years from its futile "copyright wars."[116] As commentators have widely acknowledged, confrontation and fear-mongering will not provide the desperately searched solution to address massive online copyright infringement!

Fifth, the graduated response system may be highly disproportionate.[117] As Ed Black, the president of the Computer and Communications Industry Association, observed colorfully with respect to the graduated response system: "This is not about flagrant copyright infringement, which we oppose. This is about using an Uzi to combat mosquitoes . . . ."[118] In fact, one may argue that taking away an individual's Internet access as a penalty for *alleged* copyright infringement is even worse than introducing criminal sanctions for downloading and peer-to-peer file sharing. While the criminal court system will determine whether sanctions will attach under the "beyond a reasonable doubt" standard, a graduated response system may involve *mere* allegations of infringement by copyright holders or their industry group. Indeed, as the United States Supreme Court reminded us in *BMW of North America, Inc. v. Gore*, "The principle that punishment should fit the crime 'is deeply rooted and frequently repeated in common-law jurisprudence.'"[119] The lack of proportionality in the graduated response system is, therefore, highly troubling.

Finally, the graduated response system may undermine the protection of free speech, free press, and privacy, if user activities are to be monitored and data about these activities are to be retained. One of the biggest benefits of Internet communication is anonymity. As stated in the caption of a cartoon in *The New Yorker*, "On the Internet, nobody knows you're a dog."[120] By requiring ISPs to develop a policy against alleged repeat infringers, the graduated response system invites ISPs to monitor the potentially illegal activities of Internet users. Such a system, in turn, would force ISPs to take on the role of private "proxy censors," which is inconsistent with our longstanding free speech tradition.[121] Because ISPs may

---

Vietnam).

116. For discussions of the copyright wars, see generally LESSIG, *supra* note 74; PATRY, *supra* note 17; Jessica Litman, *War and Peace: The 34th Annual Donald C. Brace Lecture*, 53 J. COPYRIGHT SOC'Y U.S.A. 1 (2006); Jessica Litman, *War Stories*, 20 CARDOZO ARTS & ENT. L.J. 337 (2002); Yu, *The Escalating Copyright Wars*, *supra* note 1; John Logie, *A Copyright Cold War? The Polarized Rhetoric of the Peer-to-Peer Debates*, FIRST MONDAY, July 7, 2003, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1064/984.

117. *See* HKSAR LEGCO PROPOSALS, *supra* note 19, at 5.

118. Juliana Gruenwald, *British Measure Cracks Down on Infringers*, NAT'L J., Apr. 8, 2010, http://techdailydose.nationaljournal.com/2010/04/british-measure-cracks-down-on.php?print=true&printcomment=1574864&print=true&print=true&print=true (internal quotation marks omitted).

119. 517 U.S. 559, 575 n.24 (1996) (quoting Solem v. Helm, 463 U.S. 277, 284 (1983)).

120. Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, NEW YORKER, July 5, 1993, at 61.

121. *See generally* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet*

need to retain information about past subscribers—and perhaps exchange information with other ISPs—in order to determine whether an individual will be considered a repeat infringer, the graduated response system may pose additional privacy concerns.[122] As Peter Hustinx, the European Data Protection Supervisor, noted in his analysis of the graduated response system:

> Such practices are highly invasive in the individuals' private sphere. They entail the generalised monitoring of Internet users' activities, including perfectly lawful ones. They affect millions of law-abiding Internet users, including many children and adolescents. They are carried out by private parties, not by law enforcement authorities. Moreover, nowadays, the Internet plays a central role in almost all aspects of modern life, thus, the effects of disconnecting Internet access may be enormous, cutting individuals off from work, culture, eGoverment applications, etc.[123]

In repressive countries with heavy information control, that policy is likely to become even more problematic.[124] If ISPs start retaining data about subscribers and their activities, they may be required to turn over such information to government authorities, who, in turn, will use the information to reconstruct the users' activities. As a result, Internet users may become reluctant to freely discuss matters (especially political ones) on the Internet. Promoted at the international level, the adoption of the graduated response system would significantly undermine our longstanding interests in promoting free speech, free press, human rights, and other civil liberties.

In sum, although the graduated response system provides considerable benefits to copyright holders, ISPs, and Internet users, the drawbacks of the system are also rather significant. It is therefore no surprise that civil liberties groups, consumer advocates, and academic commentators have widely criticized the system. In fact, given the fact that it is unclear

---

Intermediaries, and the Problem of the Weakest Link, 155 U. PA. L. REV. 11 (2006) (discussing how private actors have been enlisted as "proxy censors" to control the flow of information).

122. *See* Nimmer, *supra* note 80, at 206 (stating that "the entire enterprise of document retention [may] put[] the provider out of compliance with the laws of various jurisdictions safeguarding customer information").

123. *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) 1, 3; *see also* Ohm, *supra* note 58, at 1420 ("Internet Service Providers (ISPs) have the power to obliterate privacy online. Everything we say, hear, read, or do on the Internet first passes through ISP computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives.").

124. *See* Yu, *supra* note 31 (manuscript at 7).

whether the system's benefits would outweigh its costs, the best course of action seems not to implement the system at all.

II. DMCA

In the past two years, the entertainment industry has engaged in negotiation with ISPs to develop greater cooperation in response to illegal online file-sharing activities. On top of this cooperative agenda is the development of the graduated response system. Although the DMCA includes an ISP safe harbor and does not impose an affirmative duty on ISPs to monitor users or introduce filtering technology,[125] § 512(i) of the Copyright Act does require those ISPs that take advantage of the safe harbor to adopt and reasonably implement a policy for terminating the service of repeat infringers and to inform their users of such a policy.[126]

To strengthen their demands for cooperation with ISPs, some industry groups have suggested that the graduated response system had already been built into the DMCA framework, despite the fact that the statute was drafted in the mid-1990s and that ISPs, civil liberties groups, consumer advocates, and academic commentators have vigorously questioned the industry's position.[127] To better understand whether the graduated response system had already been built into this DMCA framework, this Part focuses on § 512(i) of the Copyright Act.

Section 512(i) specifically provides:

> (1) ACCOMMODATION OF TECHNOLOGY—The limitations on liability established by this section shall apply to a service provider only if the service provider . . . has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, 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

125. *See* 17 U.S.C. § 512(m)(1) (2006) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i) . . . ."). As Professor Nimmer noted:

> Congress was aware that allegations could assume many guises. It did not wish to saddle service providers with any duty to be pro-active in determining who is an infringer. Accordingly, it legislated that a service provider can claim immunity under Section 512 without any requirement of "monitoring its service or affirmatively seeking facts indicating infringing activity." For it is difficult or impossible to know whether "facts indicating infringing activity" will prove benign or toxic.

3 NIMMER & NIMMER, *supra* note 57, § 12B.10[B][2][b].

126. 17 U.S.C. § 502(i) (2006).

127. *Compare* Smith, *supra* note 6, *with* Sohn, *supra* note 6.

> infringers . . . .[128]

As the court declared in *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, "[T]he language of the [DMCA] and the legislative history of [§ 512(i)] are less than models of clarity."[129] According to Professor Nimmer,

> Section 512 sets forth various safe harbors for the benefit of service providers. . . . Unfortunately, the statute fails to set forth standards for meeting that policy. Even the most basic question at the heart of the statute does not lend itself to ready resolution: "No one seems to know what makes one a 'repeat infringer' . . . ."[130]

More importantly for this Article, it remains unclear whether the term "repeat infringers" would also include the *alleged* infringers that DMCA takedown notices often implicate. According to the House and Senate Reports, ISPs are "expected to adopt and reasonably implement a policy for the termination in appropriate circumstances of the accounts of subscribers of the provider's service who are repeat on-line infringers of copyright."[131] Although the Reports made it clear that the repeat infringers refer to repeat *online* infringers, they did not specify whether the provision would also cover *alleged* repeat infringers or, in the case of multiple takedown notices, *repeatedly alleged* infringers.

Indeed, the textual language in other sub-sections of § 512 seems to suggest otherwise. In his careful analysis of the provision, Professor Nimmer pointed out that Congress used different statutory language when it intended to cover *alleged* infringers, as opposed to *proven* infringers.[132]

---

128. 17 U.S.C. § 502(i).

129. 213 F. Supp. 2d 1146, 1176 (C.D. Cal. 2002).

130. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10 (quoting Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1420 (2004)); *accord* Andres Sawicki, Comment, *Repeat Infringement in the Digital Millennium Copyright Act*, 73 U. CHI. L. REV. 1455, 1462 (2006) ("The statutory term 'repeat infringer' also begs for clarification. It could refer to the number of works infringed, the number of times a work has been infringed, the number of infringing works, or the number of times an actor has been identified as an infringer.").

131. H.R. REP. NO. 105-551, pt. 2, at 61 (1998); S. REP. NO. 105-90, at 51–52 (1998).

132. *See* 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[B][2][a] ("Examination shows that, in crafting Section 512, Congress carefully delineated the difference between *allegation* and *proof*."); *see also id.* § 12B.10[B][2][a] (stating that "the statute refers to 'material or activity claimed to be infringing' among a total of twenty like references"). As Professor Nimmer explained, § 512(i) focuses narrowly on a small group of users where past conduct can be used to infer future conduct: "In order to generally exclude someone for the future, Section 512 requires certainty, not allegation . . . ." *Id.* § 12B.10[B][3][a]; *see also* Lemley & Reese, *supra* note 130, at 1420–21 ("It seems wrong . . . to say that one is an infringer merely by virtue of receiving a cease and desist letter, which some content owners have been sending with reckless abandon and which need not even meet the standards of Rule 11.").

Section 512, for example, includes the following language in its reference to alleged infringers:

- "material that is claimed to be infringing upon notification of claimed infringement";[133]
- "material or activity claimed to be infringing";[134]
- "notification of claimed infringement";[135]
- "notifications of claimed infringement";[136]
- "an exclusive right that is allegedly infringed";[137]
- "the copyrighted work claimed to have been infringed";[138]
- "the material that is claimed to be infringing";[139]
- "exclusive right that is allegedly infringed";[140]
- "claimed infringement by such faculty member";[141]
- "identification of an alleged infringer";[142]
- "identity of an alleged infringer";[143]
- "identify the alleged infringer";[144] and
- "damages . . . incurred by the alleged infringer."[145]

Thus, according to Professor Nimmer, "When Congress wished to refer to individuals who were proven infringers, it knew how to do so . . . . The meaning unmistakably denoted is those against whom infringement has been established, not against whom it is merely alleged."[146]

Moreover, an interpretation that § 512(i) already covers alleged infringers would be highly inconsistent with § 512(g), a provision that lays out the counternotice and put-back procedure. Section 512(g) limits the liability of ISPs when they restore materials that have been taken down within a period of ten to fourteen days should the complaining copyright holder not file a lawsuit.[147] As Professor Nimmer reminded us, "If notifications of claimed infringement were sufficient on their own to

133. 17 U.S.C. § 512(b)(2)(E) (2006). The ensuing list originated from Nimmer, *supra* note 80, at 175–76.

134. 17 U.S.C. § 512(f).

135. *Id*. §§ 512(b)(2)(E), 512(c)(1)(C), 512(c)(3)(A), 512(d)(3).

136. *Id*. §§ 512(c)(2), 512(e)(1)(B).

137. *Id*. § 512(c)(3)(A)(i).

138. *Id*. § 512(c)(3)(A)(ii).

139. *Id*. § 512(c)(3)(A)(iii).

140. *Id*. § 512(c)(3)(A)(vi).

141. *Id*. § 512(e)(1)(B).

142. *Id*. § 512(h)(1).

143. *Id*. § 512(h)(2)(C).

144. *Id*. § 512(h)(3).

145. *Id*. § 512(f).

146. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[B][3][b].

147. 17 U.S.C. § 512(g) (2006).

establish infringement, no put-back and counter-notification provision would have needed to be included in the statute."[148]

Notwithstanding Congress's full intent to limit the provisions' coverage to proven infringers, a fair question remains as to how repeat infringers are to be defined. Notably, the word "repeat" has not been used elsewhere in Title 17 of the United States Code.[149] One therefore needs to interpret the word "repeat" by reference to its variants, such as the word "repeated." In his analysis of § 512(i), Professor Nimmer began with the *Oxford English Dictionary* and defined the term "repeat" to mean "doing something for a second time or duplicating it."[150] (This definition actually implies that the graduated response system exceeds the minimum by requiring a repeat infringer to do something a *third* time.)

Nevertheless, Professor Nimmer went on to point out that both the House and Senate Reports reflected Congress's understanding that "there are different degrees of on-line copyright infringement, from the inadvertent and noncommercial, to the willful and commercial."[151] The Reports stated further that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access."[152] According to Professor Nimmer, "The use of the word 'flagrantly' suggests that the infringement must be shocking or notorious. Accordingly, the legislative history suggests that Congress had in mind a policy that would focus on egregious offenders, rather than on casual two-time offenders."[153]

---

148. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[B][3][b]; *see also* Nimmer, *supra* note 80, at 196 ("The very existence of the counter-notification and put-back procedures emphasizes that notices are no more than rebuttable accusations of infringement. Accordingly, if a subscriber or account holder is accused of copyright infringement and challenges that accusation, then the subscriber or account holder cannot be considered an 'infringer' until a court has adjudicated him to deserve that label.").

149. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[C] ("In the entire Copyright Act, the instant policy contains the only instance of the word 'repeat.'").

150. *Id.* § 12B.10[C][1] (referencing without quoting the *Oxford English Dictionary*).

151. H.R. REP. NO. 105-551, at 61 (1998); S. REP. NO. 105-90, at 52 (1998).

152. H.R. REP. NO. 105-551, at 61 (1998); S. REP. NO. 105-90, at 52 (1998).

153. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[C][2]. As Professor Nimmer continued: "[A] *repeat* infringer would appear to be one who has infringed copyrights at two different times. Accordingly, a party's infringement of multiple copyrights simultaneously does not render him a 'repeat infringer.' The latter act would not be repeat infringement, but instead a single act of infringement of multiple copyrights." *Id.* § 12B.10[C][1]; *see also* Bridy, *supra* note 50 (manuscript at 50) ("When it comes to adding up strikes, ISPs should count a single notice of infringement that alleges multiple instances of infringement as only one 'strike' against the subscriber receiving the notice. To do otherwise would effectively take the 'graduated' out of graduated response and would undermine the rehabilitative principle that infringing consumers should be given repeated opportunities to reform and comply.").

If one is willing to revisit the House and Senate Reports on the 1976 Act, one may find additional support for this interpretation. In explaining the use of the term "repeated" in § 111 of the Copyright Act—a provision concerning secondary transmissions in the cable system—the House Report declared: "'Repeated' does not mean merely 'more than once,' of course; rather, it denotes a degree of aggravated negligence which borders on willfulness."[154] Although this explanation was written more than two decades before the enactment of § 512 and given that Congress was unlikely to have anticipated the challenges brought about by the Internet and new communications technologies, it is not far-fetched to suggest that the word "repeat" in § 512(i) means more than "doing something for a second time or duplicating it." Instead, it makes good sense that the word "repeat" means something more serious—something that "denotes a degree of aggravated negligence which borders on willfulness."

To be certain, while most people would argue that *uploading* hundreds or thousands of copyrighted songs and movies for others to download reflects such "a degree of aggravated negligence" or a "flagrant" abuse of their Internet access, it remains arguable whether *downloading* the same number of songs and movies would be viewed the same.[155] Indeed, many civil liberties groups, consumer advocates, and academic commentators would point out that the current copyright law may be inconsistent with existing social norms and community values,[156] especially among the so-called "digital natives" who were born after the arrival of the Internet and the "digital migrants" who made successful transition to the Internet.[157] Both groups are likely to find rules against free sharing of online content counterintuitive. As Professor Mark Lemley reminded us: "[I]f a law is so out of touch with the way the world works that it must regularly be ignored in order for the everyday activities of ordinary people to continue, perhaps

154. H.R. REP. NO. 94-1476, at 93 (1976).

155. *See* Yu, *supra* note 31 (manuscript at 28) (discussing the distinction between uploading, downloading, and peer-to-peer file-sharing in the consultation documents concerning digital copyright reform in Hong Kong).

156. As Fred von Lohmann observed:

> By conservative estimates, 1 in 5 American Internet users is an active file-sharer. Does the recording industry really think that banning 20% of Americans from the Internet is the right answer? Do ISPs? Or will the millions of ISP "warnings" just give rise to more encrypted and anonymized file-sharing mechanisms, all the while getting no artists paid?

von Lohmann, *supra* note 30.

157. JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008) (describing generational differences in the use of digital technology and the Internet); *see also* Yu, *P2P and the Future*, *supra* note 1, at 756–63 (discussing massive online copyright infringement in relation to Generation Y).

we should begin to question whether having the law is a good idea in the first place."[158]

Regardless of one's view on the file-sharing issue, which involves the unauthorized reproduction and distribution of verbatim copies of copyrighted files, however, the creative reuse of copyrighted materials in the context of user-generated content[159] presents a much harder case. While

158. Mark A. Lemley, *Dealing with Overlapping Copyrights on the Internet*, 22 U. DAYTON L. REV. 547, 578 (1997); *see also* Stuart P. Green, *Plagiarism, Norms, and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights*, 54 HASTINGS L.J. 167, 238 (2002) ("People whose internal moral codes would never allow them to walk into a store and steal a piece of merchandise apparently think there is nothing wrong with making an unauthorized copy of a videotape or downloading a bootlegged computer program."); Geraldine Szott Moohr, *Defining Overcriminalization Through Cost-Benefit Analysis: The Example of Criminal Copyright Laws*, 54 AM. U. L. REV. 783, 795 (2005) ("Under any theory of deterrence, it is more difficult to induce law-abiding behavior when underlying social norms do not support the law. Simply put, people are more likely to obey criminal laws that reflect community values or moral judgments of right and wrong."). As Professor Geraldine Moohr elaborated further:

> Criminal enforcement actions that impose harsh penalties for conduct that is not viewed as immoral or harmful can lower the community's respect for the criminal law and thereby diminish both its legitimacy and its general effectiveness. People who have not internalized the legal standard may obey the law because they respect its legitimacy, even when social norms are in transition. But if respect and legitimacy are diminished, people will be less likely to obey or to impose informal sanctions on others.
>
> Respect and legitimacy are threatened when a community norm that condemns prohibited conduct is not yet in place. In that situation, criminal enforcement coupled with severe penalties can make pawns of those caught in the transition period and offend community notions of due process, fairness, and commonly held ideas about notice and legality. If the community believes these severe sanctions are disproportionate to the offense, especially if only a small percentage of personal infringers are targeted, then enforcing criminal infringement crimes may be detrimental. To the extent that citizens reject rules that target people unfairly, they may similarly reject the legal system that promulgates and enforces such rules. In these circumstances, enforcing rules that do not embody a shared community norm may actually undermine the formation of a norm against the forbidden conduct.

Id. at 804–05. *But see* Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-based Business Models*, 22 CARDOZO ARTS & ENT. L.J. 725, 735 (2005) ("[I]f awareness of a law has risen dramatically, but compliance has not, the law enters a window of vulnerability where compliance must rise or the law will fall into disrespect. (It was not disrespected when no one knew about it.)").

159. Commentators and industry representatives have questioned the term "user-generated content." *Compare* Alan N. Braverman & Terri Southwick, *The User-Generated Content Principles: The Motivation, Process, Results and Lessons Learned*, 32 COLUM. J.L. & ARTS 471, 471 (2009) ("UGC . . . is not always user-generated; it would more accurately be called user-posted content."), *and* Daniel Gervais, *The Tangled Web of UGC: Making Copyright Sense of User-Generated Content*, 11 VAND. J. ENT. & TECH. L. 841, 842 (2009) ("Let me be perfectly clear: there is no such thing as 'user-generated content.'"), *with* Steven Hetcher, *User-Generated Content and the Future of Copyright: Part One—Investiture of Ownership*, 10 VAND. J. ENT. & TECH. L. 863, 870–74 (2008) (providing a definition of the user-generated content).

civil liberties groups, consumer advocates, and academic commentators insist on their legality (or at least the need for copyright reform to legalize such use),[160] some copyright holders concede their lack of interest in taking action against those creations, despite their unauthorized nature.[161] For many user-generated contents, there is also a fair and valid question concerning whether the content's transformative nature would warrant favorable consideration in a fair use analysis.[162] Indeed, it would seem highly problematic that the rights consumers traditionally enjoy in the physical space—such as fair use—have not been built into the graduated response system.

In sum, although some in the entertainment industry have suggested that the graduated response system had already been built into the DMCA framework, it is blatantly clear that Congress did not intend the provision to cover *alleged* infringers. Nor did the legislators have the graduated response system in mind when they drafted § 512(i). In fact, as the United States Court of Appeals for the District of Columbia Circuit aptly noted in *Recording Industry Association of America v. Verizon Internet Services*,[163] "P2P software was 'not even a glimmer in anyone's eye when the DMCA was enacted.' . . . [N]or did [Congress] draft the DMCA broadly enough to reach the new technology when it came along."[164]

In fact, in an interview in December 2008, Cary Sherman admitted that the RIAA and the ISPs had been "actively engaged in discussions for

160. Commentators have discussed the many benefits of user-generated contents. Professor Greg Lastowka, for example, noted: "[U]ser-generated content allows the collective mind of the audience to criticize and personalize popular narratives. . . . [F]rom the standpoint of liberal democracy, user-generated (or 'peer produced') content [also] offers an improvement over the past hierarchical models of information production and distribution." Greg Lastowka, *User-Generated Content and Virtual Worlds*, 10 VAND. J. ENT. & TECH. L. 893, 899–900 (2008).

161. As Professor Tim Wu explained, such unauthorized use is better described as "tolerated use":

> Tolerated use is infringing usage of a copyrighted work of which the copyright owner may be aware, yet does nothing about. There may be a variety of reasons for tolerating use. Reasons can include simple laziness or enforcement costs, a desire to create goodwill, or a calculation that the infringement creates an economic complement to the copyrighted work—it actually benefits the owner.

Tim Wu, *Tolerated Use*, 31 COLUM. J.L. & ARTS 617, 619 (2008).

162. *See generally* Rebecca Tushnet, *User-Generated Discontent: Transformation in Practice*, 31 COLUM. J.L. & ARTS 497, 497 (2008) (discussing how "nonlawyers' concepts of transformativeness [in the context of user-generated content] could enrich legal understandings of the appropriate boundaries of fair use").

163. 351 F.3d 1229 (D.C. Cir. 2003).

164. *Id*. at 1238 (quoting *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 38 (D.D.C. 2003)); *see also* Urban & Quilter, *supra* note 82, at 686–87 ("Peer-to-peer and other distributed networks were not anticipated by policymakers during the crafting of § 512, and in a world where valuable copyright properties are distributed without 'hosting' ever occurring, the notice-and-takedown provisions under § 512(c) seem less likely to be of use to the very copyright industry groups that helped compromise on the question of OSP liability during the legislative process.").

[only] about a year."[165] Nevertheless, there is no denial that some colleges, universities, and ISPs have already put in place their individual graduated response system.[166] The Higher Education Opportunity Act of 2008 also has contributed to such developments, by conditioning the receipt of federal financial aid on the development of "plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents."[167] The implementing regulations, which took effect July 2010, further require the implementation of these plans.[168]

III. THOUGHT EXPERIMENTS

In an earlier article written when the recording industry began filing lawsuits against individual file-sharers, I laid out three different thought experiments to explain why policymakers who seek to address massive online copyright infringement should complement legal solutions with others that take account of market forces, technological architectures, and social norms.[169] Those experiments seek to challenge policymakers and commentators to step outside their mental boundaries to rethink the peer-to-peer file-sharing debate.

This Part uses the same approach and introduces three thought experiments to highlight the problems and unintended consequences the graduated response system would bring about. These thought experiments focus on three areas that will remain important in the ongoing development of digital copyright law: (1) the emergence of user-generated content, (2) the protection of free speech and free press, and (3) the retention of the fair use privilege in copyright law.

---

165. Anderson, *supra* note 4 (quoting Cary Sherman, president of the RIAA).

166. As Cary Sherman observed:

> Colleges and universities have really been engaged in their own form of graduated response for many years. If you take a look at what universities have been doing, they have escalating sanctions for people who have been identified as repeat infringers. Something as simple as, for example, at Stanford, where they charge a $100 reconnection fee for somebody who fails to respond to a first notice. Then a second offense is $500 and a third [time] offender has network privileges terminated and to regain access, they have to pay a $1,000 fee. That's a very clear graduated response system.
>
> Others will just give a warning the first time, and the second time they might do a temporary disconnect for 24 hours, and a third time they might refer you to the judicial affairs system. Every school has its own variation, but they've really been implementing informal graduated response.

Id. (quoting Cary Sherman, president of the RIAA). In addition, "some ISPs, including Cox Communications, established antipiracy policies long ago that were similar to the RIAA's graduated response." Sandoval, *supra* note 41.

167. 20 U.S.C. § 1094(a)(29)(A) (Supp. II 2009).

168. 34 C.F.R. § 668.14 (2009). Thanks to Professor Bridy for pointing this out.

169. *See* Yu, *P2P and the Future*, *supra* note 1, at 744–63.

A. *User-Generated Content*

The first thought experiment concerns the prepublication video identification system YouTube has developed to enable copyright holders to decide for themselves whether they want to monitor, monetize, or stop the unauthorized distribution of their content. As William Patry described:

> A motion picture studio or other audiovisual content owner provides YouTube with a file of its work. YouTube then encodes the file; when a third party attempts to upload content that provides a match, YouTube contacts the studio and asks the studio what steps it wants to take. The studio can decide to block the upload, let the file be uploaded but tracked, or let the file be uploaded and run either contextual or its own advertisements against it, with the revenues generated being shared. An estimated 90 percent of content owners using video content identification have chosen to monetize their works, resulting in revenues that would not otherwise have been received. Even before the development of its video content identification, YouTube had in place a similar system for audio content contained in consumer-created videos, with an additional feature: Where an audio content owner objects to the use of the music, YouTube offers the user who created the video the ability to engage in an "audio swap." YouTube will, if requested, strip out the objected-to audio and replace it with a song that either is in the public domain or licensed, thereby leaving the user-generated, noninfringing video up for viewing, while respecting copyright owners' rights. These systems are a win-win . . . .[170]

From the standpoint of both rights holders and consumers, this prepublication system seems to be a major improvement over the graduated response system, the individual lawsuits, and the occasional criminal prosecutions. By allowing copyright holders to determine for themselves their preferred response, this prepublication system struck a better balance in copyright law, notwithstanding the potential fears of greater corporate influence on, if not control over, culture.

Unfortunately, those ISPs that take a zero tolerance approach or deploy an inflexible "three strikes" system will not support this prepublication system. Instead, the violative users will be shut down despite the fact that some copyright holders may be willing to allow the unauthorized use to continue. Even if the "three strikes" system could take the rights holders'

170. PATRY, *supra* note 17, at 38–39; *see also* Claire Cain Miller, *YouTube Ads Turn Videos into Revenue*, N.Y. TIMES, Sept. 3, 2010, at B1, *available at* 2010 WLNR 17553433 (providing examples of how YouTube has enabled copyright holders to receive advertising revenues for the unauthorized distribution of their videos).

preferences into account, the system would create inequitable results that require the shutting down of *some* users but not the others.

A graduated response system that takes copyright holders' preferences into account is no longer a system that separates authorized use from its unauthorized counterpart. Rather, it recognizes an intermediate category of uses, which Professor Tim Wu described as "tolerated use"—a term he coined to reflect the "infringing usage of a copyrighted work of which the copyright owner may be aware, yet does nothing about."[171] Professor Edward Lee further introduced the idea of hedging to cover a broader set of uses, which include "tolerated use, acquiesced use, accepted use, publicly encouraged use, and uses that even might be supported by implied licenses."[172] As he explained: "The advantage of hedging . . . is that copyright holders can get the best of both worlds: free promotion and talent trolling from various unauthorized uses of their works, combined with the ability to later protest other unauthorized uses of their works."[173]

While it is not a bad idea to institute a system that *tolerates* unauthorized use, and copyright law always involves a certain amount of toleration, a system that disconnects or penalizes users based on the individual preferences or tolerance levels of selected copyright holders seems rather unfair and undemocratic. By making it difficult for users to adjust their online behavior and learn from their mistakes, such a system is also likely to promote uncertainty. As Professor Sonia Katyal wrote:

> [T]he confluence of . . . overbroad piracy surveillance . . . [and] tolerated uses . . . suggests a continuing degree of uncertainty. The result is a pervasive divide between what the law requires, and what the market tolerates, leaving consumers open to an unpredictable interpretation of their activities, and an even deeper vulnerability than the DMCA intended.[174]

Moreover, by allowing one powerful copyright holder, or its even more powerful trade group, to disrupt a user's connection, the graduated response system will have created in that particular copyright holder veto power over the choices of other less powerful copyright holders, who may choose to tolerate the unauthorized use and thereby benefit from such exploitation—through advertising revenues, perhaps. After all, users cannot be disconnected in response to a complaint by *one* right holder

171. Wu, *supra* note 161, at 619; *see also* Edward Lee, *Warming up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1486–88 (2008) (discussing hedging by copyright holders when they have a wait-and-see attitude toward the different uses of their works).

172. Lee, *supra* note 171, at 1488.

173. *Id*. at 1486–87.

174. Sonia K. Katyal, *Filtering, Piracy Surveillance and Disobedience*, 32 COLUM. J.L. & ARTS 401, 418 (2009).

while at the same time retaining an Internet connection to exploit those works whose unauthorized use has been tolerated by *others*.

B. *Free Speech and Free Press*

The second thought experiment involves online news postings from a major newspaper, such as *The New York Times* or *The Washington Post*. There is no doubt that such postings receive some of the highest protections under either the First Amendment in the United States[175] or Article 10 of the European Convention of Human Rights in the European Union.[176] Notwithstanding these important and well-deserved protections, and society's strong interests in accommodating free speech and free press protections within the copyright system,[177] the protection of journalists under a graduated response system remains suspect. Such limited protection would affect not only the mainstream journalists, but also online journalists, bloggers, and those unconventional websites that bring us news through digital media.

Interestingly, although the entertainment industry has pushed strongly for the development of a graduated response system, it remains unclear whether all of its member companies would actually benefit from such a

---

175. *See* U.S. CONST. amend. I.

176. *See* Strowel, *supra* note 2, at 83 ("[O]ne can expect that the European Court of Human Rights would not consider the internet suspension of a journalist account as indispensable and proportionate, as the European Court is very much opposed to any broad limitation of the free expression of journalists."). Article 10 of the European Convention of Human Rights provides:

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 221; *see also* Peter K. Yu, *Reconceptualizing Intellectual Property Interests in a Human Rights Framework*, 40 U.C. DAVIS L. REV. 1039, 1096–99 (2007) (discussing the tension between copyright protection and the protection offered under Article 10 of the European Convention of Human Rights).

177. *See* Eldred v. Ashcroft, 537 U.S. 186, 219 (2003) (underscoring the various "built-in First Amendment accommodations" in existing copyright law); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985) (stating that the Framers of the Constitution intended copyright to be the "engine of free expression"); Ashdown v. Tel. Group Ltd., [2001] EWCA (Civ) 1142 (Eng.) (balancing copyright protection against the protection of freedom of expression).

system. Nor is it likely that these members would express strong support for the system had they fully understood that the system could backfire on them. As Professor Nimmer observed with respect to the § 512(i) repeat infringer provision: "One might expect that a copyright owner such as Twentieth Century Fox would, at a bare minimum, urge that a party who has been adjudicated a deliberate infringer on multiple occasions would qualify; but, on inspection, even that expectation turns out to be wrong."[178] As he explained:

> For those studios themselves are the frequent targets of infringement lawsuits—indeed, the price for a successful film typically includes multiple suits brought by the "true" originator of the script (regardless of their own conflicting claims!) who has been "deliberately ripped off" by heartless Hollywood; a few of those claims actually succeed. But it only takes a few to tar each studio as a "repeat infringer" if no further thought goes into the calculus. Indeed, already by 1940, MGM had suffered two strikes for deliberate infringement, one at the Supreme Court level. A similar story applies to the other studios. As litigation has grown over the decades, the tally of adjudicated infringements as to every studio has only grown.
>
> The language [in a repeat infringer policy could] remit a strike when evidence exists that a subscriber infringed "unintentionally or in the good faith belief that its conduct did not constitute infringement, or that the adjudicating court considered the issue of infringement to be open to divergent interpretations." Yet even that language is not enough to protect the MGMs and Foxes of the world, inasmuch as their conduct is occasionally ruled deliberate, and twice is all it takes.[179]

178. Nimmer, *supra* note 80, at 170.

179. *Id*. at 216–17. As Professor Nimmer pointed out:

> MGM lost suits as to the films *Letty Lynton*, see Sheldon v. Metro-Goldwyn Pictures Corp., 309 U.S. 390, 397 (1940) . . . and *A Day at the Races*, see Barsha v. Metro-Goldwyn-Mayer, 90 P.2d 371 (Cal. Ct. App. 1939). . . .
>
> For example, Twentieth Century Fox suffered defeat as to *Captain January*, not to mention *The Lieutenant Wore Skirts*. *See* L.C. Page v. Fox Film Corp., 83 F.2d 196, 199 (2d Cir. 1936); Fader v. Twentieth Century-Fox Film Corp., 169 F. Supp. 880, 881[, 882] (S.D.N.Y. 1959). Turning to Universal, the famous cases that immediately come to mind concern its infringement arising out of *Rear Window*, *Battlestar: Galatica*, and *12 Monkeys*. *See* Stewart v. Abend, 495 U.S. 207 (1990); Twentieth Century-Fox Film Corp. v. MCA, Inc., 715 F.2d 1327 (9th Cir. 1983); Woods v. Universal City Studios, Inc., 920 F. Supp. 62 (S.D.N.Y. 1996).

Nimmer, *supra* note 80, at 216–17 nn.225–26.

Thus, if such infringements involve online materials, these studios very well may fit within the definition of "repeat infringers" under § 512(i). Their Internet service, as a consequence, would be vulnerable to disconnection—perhaps in response to takedown notices sent by their competitors or disgruntled former employees.

Like these studios, newspapers may lose their Internet service if they include online, on at least two occasions, plagiarized reports that infringed on others' copyrighted works.[180] Because of these infringing activities, the newspapers would be identified as "repeat infringers" within the meaning of § 512(i). The newspapers might also be considered *alleged* infringers if their competitors seek to use takedown notices to interrupt their service. Under such a scenario, the newspapers will be subject to Internet disconnection just like individual file-sharers.

Although newspapers and broadcasters are generally believed to be highly vulnerable to copyright lawsuits—thus warranting special and differential treatment of innocent infringers[181]—the Internet service of a major newspaper is unlikely to be suspended for at least four reasons. First, because the newspaper can afford to pay damages in a civil action, copyright holders may prefer to sue for monetary damages or obtain a handsome settlement. They therefore have very limited interest in actually disrupting the newspaper's Internet service (unless such disruption could enhance the likelihood or amount of settlement).

Second, the harm caused by the disconnection may greatly outweigh the benefits of protecting the relevant copyright holder. Given the highly disproportionate nature of Internet disconnection when the sanction was compared against the damage caused by the posting of potentially infringing reports, the newspaper's lawyers may succeed in obtaining an injunction from court to protect the newspaper's Internet service.

Moreover, to put the number of infringements in the right context, that number needs to be measured against the number of lawsuits a user is confronted with on a regular basis and how vulnerable he or she is to copyright lawsuits. As Professor Nimmer observed: "If a Hollywood studio wins a hundred such suits but loses two in a decade, it scarcely seems to

---

180. There may be additional questions concerning when and whether a company should be considered a repeat infringer when its employees post or e-mail infringing material using the company's e-mail and Internet access. As Professor Nimmer asked:

> Does it matter if the employee was acting outside the scope of his employment? What if an infringing executive later leaves her employ—does the company get a clean slate after the executive's departure? Concomitantly, if that executive leaves to join another company, does she carry her repeat infringer status with her such that it can be attributed to the new company?

Nimmer, *supra* note 80, at 210.

181. *See* H.R. REP. NO. 94-1476, at 163 (1976) (stating that "broadcasters and newspaper publishers . . . are particularly vulnerable to [the] type of infringement suit [where the infringer was not aware and had no reason to believe that its acts constituted an infringement of copyright]").

fall within Congress's contemplation as a 'repeat infringer' that forever deserves to be defrocked."[182]

A key problem with the graduated response system is its failure to view the number of infringements in comparison to the overall amount of legal use. It ignores the fact that the creation of some highly socially desirable copyrighted works may involve more risks of infringement than the creation of other works. The system also fails to take into account the fact that having infringed twice over a period of three months is quite different from having the same number of infringements over, say, a decade.

Third, because the newspaper is likely to be one of the ISP's main customers, the ISP may be very reluctant to suspend its service. Suspending the service of such a major customer could cause incalculable harm to the ISP both financially and in terms of public relations. Instead, the ISP may choose to continue to provide the service by emphasizing the phrase "in appropriate circumstances" as a limitation in § 512(i) while at the same time citing the public interest of news reporting as well as the financial hardship for which the provider would suffer. Moreover, although the lack of suspension may open the ISP to further liability, the ISP, in this case, is likely to be able to indemnify the newspaper for any damages it suffers or, in the alternative, purchase insurance to protect itself.

Finally, the ISP may be owned by the newspaper or be a subsidiary of a parent company that owns both the ISP and the newspaper. Such a scenario is actually rather common in today's highly concentrated media environment—in both the United States and other parts of the world.[183] Before its disintegration, AOL Time Warner provided a leading example of such a combination. If approved, Comcast's takeover of NBC Universal will provide another good example.

Although the ISP's nonsuspension of the newspaper is, in the view of most people, a *correct* result, the different treatment between this major newspaper and individual file-sharers is rather disturbing. Such difference is the direct, or at least partial, result of a system that favors those who have deep pockets over those others who have limited resources to either respond to copyright lawsuits or to put pressure on the ISP to keep their service. A system that penalizes consumers for their "shallow pockets" seems highly inequitable.

---

182. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[F] n.129; *see also* Sawicki, *supra* note 130, at 1482 ("[A] consumer-infringer who has downloaded two movies over the course of ten years should not be treated the same way as a consumer-infringer who has downloaded several dozen in a single month.").

183. For discussions of growing media concentration, see generally BEN H. BAGDIKIAN, THE MEDIA MONOPOLY (6th ed. 2000); ROBERT W. MCCHESNEY, RICH MEDIA, POOR DEMOCRACY: COMMUNICATION POLITICS IN DUBIOUS TIMES (1999).

C. *Fair Use*

The last thought experiment concerns the use of copyrighted materials in a way that has been found to be fair use in *some* jurisdictions but infringement in *other* jurisdictions. Such a scenario actually occurs more often than we expect. Fair use is notoriously complex, elusive, and unsettled. As declared in *Dellar v. Samuel Goldwyn, Inc.*, the fair use doctrine is "the most troublesome in the whole law of copyright."[184] Because ISPs are likely to err on the side of copyright protection, the graduated response system may choose to consider the user an infringer, as opposed to a fair user in this scenario.

To complicate matters, the current technology is unable to capture the full range of exceptions and limitations in the copyright system. Commentators, for example, have pointed out the considerable mismatch between technology and fair use. As Professor Edward Felten noted, "Fair use is one of the starkest examples of the mismatch between what the law requires and what technology can do. Accurate, technological enforcement of the law of fair use is far beyond today's state of the art and may well remain so permanently."[185] Indeed, as he described colorfully in the context of digital rights management, a technological measure "that gets all fair use judgments right would in effect be a 'judge on a chip' predicting with high accuracy how a real judge would decide a lawsuit challenging a particular use. Clearly, this is infeasible with today's technology."[186]

---

184. 104 F.2d 661, 662 (1939) (per curiam); *see also* MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW § 10.02, at 470 (4th ed. 2005) (stating that the fair use privilege is "an elusive legal doctrine, reputed to be the most troublesome in copyright law"); Jacqueline D. Lipton, *Solving the Digital Piracy Puzzle: Disaggregating Fair Use from the DMCA's Anti-device Provisions*, 19 HARV. J.L. & TECH. 111, 121 (2005) ("Fair use has always been a problematic concept within copyright law. Although it is an important defense against a claim of copyright infringement, its precise boundaries have never been clear.").

185. Edward W. Felten, *A Skeptical View of DRM and Fair Use*, COMM. ACM, Apr. 2003, at 57, 59; *see also* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 56 (2001) ("At least for now, there is no feasible way to build rights management code that approximates both the individual results of judicial determinations and the overall dynamism of fair use jurisprudence."); Ian R. Kerr et al., *Technical Protection Measures: Tilting at Copyright's Windmill*, 34 OTTAWA L. REV. 7, 31 (2002) ("[T]he technologies employed by DRMs are not yet sufficiently sophisticated to mirror the law of copyright because TPMs themselves remain incapable of distinguishing between infringing and non-infringing uses of digital works."); R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619, 629 (2003) ("Technological protection measures that control reproduction or performance of a work, however, are unlikely to be well calibrated to the actual contours of, for example, copyright owners' reproduction or public performance rights.").

186. Felten, *supra* note 185, at 58; *see also* Burk & Cohen, *supra* note 185, at 55 (expressing their pessimism over the ability of "system designers . . . to anticipate the types of uses that would be considered fair by a court"); *id.* at 59 ("At present, only human intelligence, reviewing the unique circumstances of a particular use, can determine whether it is likely to be fair.").

The fact that one cannot enjoy and exercise fair use protection that is duly recognized in the copyright statute is highly troubling. It is therefore no surprise that commentators have noted the importance of protecting fair use rights as affirmative rights.[187] It is also worth considering whether innocent users can obtain compensation from their ISPs, which often include the right to interrupt or terminate service in their terms of service while providing immunity clauses that shield themselves from lawsuits for damages caused by such interruption or service termination.[188] In addition, it is worth exploring whether the user could obtain compensation from those copyright holders who make unfounded accusations that lead to wrongful suspensions.

Procedural safeguards and substantive compensation along the line of § 512(f), which penalizes those who "knowingly materially misrepresent[]" information,[189] may help alleviate some of these concerns. Nevertheless, that quoted phrase is in desperate need of modification in light of the fact that "copyright's ambiguity assures that many statements of infringement can be made in good faith, even though a court may find that no infringement actually exists."[190] To protect users from overzealous enforcement and imprecise technology, it may also be helpful to develop a compensation pool with contributions from rights holders and ISPs. Such a pool can be used to pay for damages Internet users suffer when their service has been wrongfully disrupted or terminated.

IV. BASIC PRINCIPLES

Parts I.B and III explain why a graduated response system that is not carefully tailored to the needs of Internet users and that focuses on *alleged* infringers, as opposed to *proven* infringers, is highly undesirable. By contrast, Part I.A demonstrates the substantial benefits a well-crafted graduated response system may provide to copyright holders, ISPs, and

187. These user rights include, among others, first sale rights and fair use rights. *See* Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 381 n.74 (1997); *see also* Rochelle Cooper Dreyfuss, *TRIPS—Round II: Should Users Strike Back?*, 71 U. CHI. L. REV. 21, 27 (2004) ("User access did not need specific delineation when it was the background rule; only the exceptionalism of intellectual property rights required express definition. But if the new background is proprietary control, then the exceptionalism of user rights now needs to be embedded into positive law."); Peter K. Yu, *TRIPs and Its Discontents*, 10 MARQ. INTELL. PROP. L. REV. 369, 396–401 (2006) (discussing the need to add explicit access rights to the TRIPS Agreement).

188. *See* Urban & Quilter, *supra* note 82, at 629.

189. 17 U.S.C. § 512(f) (2006).

190. Yen, *supra* note 46, at 1888 n.278 ("Some may argue that the DMCA alleviates the problem of indiscriminately removing speech from the Internet by providing for penalties against those who make knowingly false representations about the existence of infringement. This argument misses the mark because 'knowing' misrepresentations do not include statements that are made in good faith but incorrect about the existence of infringement. Indeed, copyright's ambiguity assures that many statements of infringement can be made in good faith, even though a court may find that no infringement actually exists." (internal citation omitted)).

even Internet users. Recognizing the serious harm created by repeat online infringers, this Part seeks to reconcile the tension raised by these different Parts of the Article.

To begin with, policymakers should not adopt a graduated response system unless sufficient proof exists to show that the system is needed and that the system will meaningfully reduce online copyright infringement.[191] In economic terms, the benefits of the graduated response system should outweigh its costs. Such a cost-benefit analysis should take into account both the local conditions and the challenges in quantifying such costs as harm to free speech, free press, privacy, and other civil liberties.

If the introduction of a graduated response system is unavoidable, due to either heavy foreign pressure or significant local benefits, seven basic principles should be built into this system, regardless of whether the system is mandated by law or introduced through private contracts. This Part outlines each of these principles. Taken together, the principles aim to set the needed parameters to enable the copyright system to strike an appropriate balance among the interests of copyright holders, ISPs, and Internet users.

A. *Independent Review*

The graduated response system should include an independent review mechanism. Such a mechanism is particularly important in light of the many technological problems inherent in the identification process as well as the unavoidable good-faith misjudgments of laws by anxious copyright holders and their even more anxious agents. As the district court wrote in *Corbis Corp. v. Amazon.com, Inc.*, "A copyright owner may have a good faith belief that her work is being infringed, but may still be wrong. . . . [T]hird party notices [therefore] do not, in themselves, constitute red flags."[192] Likewise, in the trademark context, a district court stated in *Tiffany (NJ) Inc. v. eBay, Inc.* that the takedown notice "was not a notice of actual infringement, but instead, was a notice of [the right holder's] good-faith belief that a particular item or listing was infringing."[193]

Although technology has advanced significantly to reduce the number of false positives, the suspension of something as important as Internet service for a fixed period of time is no trivial matter. If the system is to be considered fair and legitimate, and the rule of law is to be respected, the

191. *See* Peter K. Yu, *The International Enclosure Movement*, 82 IND. L.J. 827, 901 (2007) (noting the need to "require impact studies before a further expansion of intellectual property protection"); *see also* Yu, *supra* note 36, at 50–54 (lamenting the lack of sufficient empirical proof to "conclusively demonstrate whether an anticircumvention regime will be expedient, or even needed, in less developed countries").

192. 351 F. Supp. 2d 1090, 1105, 1108 (W.D. Wash. 2004).

193. 576 F. Supp. 2d 463, 515 n.38 (S.D.N.Y. 2008).

infringing activities of those who stand to lose Internet service must be verified through an independent review process.

This process can be introduced through either the judicial process or via an administrative mechanism.[194] If an administrative mechanism is used in lieu of a judicial process, the mechanism should only be used against those who have been convicted once—and preferably twice—in a court of law. The right to be heard is an important procedural safeguard that was built into the legal system to protect the innocent. This right should not be easily given up even amidst massive online copyright infringement.

B. *Educative and Rehabilitative Benefits*

The graduated response system needs to take seriously its educative and rehabilitative roles.[195] For example, the system should focus on the type of infringement that is understandable by Internet users with limited knowledge of copyright law.[196] In order for the infringing activities to constitute repeat infringement, the activities should consist of a *similar* type of infringement. In addition, to provide the needed educational benefits, there should be sufficient lag time between notices,[197] not to

194. *See* Lemley & Reese, *supra* note 130, at 1351 (advocating the development of a "quick, cheap dispute resolution system that enables copyright owners to get some limited relief against abusers of p2p systems and to deter others from such abuse"); Lipton, *supra* note 184, at 116–17 (proposing the introduction of a complaint and enforcement procedure to facilitate legitimate uses of copyrighted works that are "locked up" by copy-protection technologies); Yu, *supra* note 31 (manuscript at 51) (articulating the need to "introduce a complaint and enforcement procedure to examine and respond to cases where the OSP fails to put back materials on a timely basis following the receipt of a counter notice"). As Professors Lemley and Reese explained, the development of an administrative mechanism is sometimes necessary:

> It seems wrong, though, to say that one is an infringer merely by virtue of receiving a cease and desist letter, which some content owners have been sending with reckless abandon and which need not even meet the standards of Rule 11. The other extreme—that one is not an infringer until adjudicated so by a court, and so repeat infringers must be sued to final judgment and lose twice—seems equally unworkable. The administrative procedure provides a middle ground, by allowing a relatively quick determination by a neutral third party that an individual is in fact an infringer. Keying the termination obligation to an administrative finding would protect the due process rights of those wrongfully accused of infringement without rendering the repeat infringer provision virtually ineffective.

Lemley & Reese, *supra* note 130, at 1420–21.

195. *Cf.* Strowel, *supra* note 2, at 86 (highlighting "the educational effect of the warnings").

196. *Cf.* Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19, 39 (1996) ("We can continue to write copyright laws that only copyright lawyers can decipher, and accept that only commercial and institutional actors will have good reason to comply with them, or we can contrive a legal structure that ordinary individuals can learn, understand and even regard as fair.").

197. *Cf.* 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[C][1] ("[A] party's infringement of multiple copyrights simultaneously does not render him a 'repeat infringer.' The latter act would not be repeat infringement, but instead a single act of infringement of multiple copyrights.").

mention that each notice should be delivered in a way that provides *actual* notice to the relevant user.[198]

In fact, if infringers cannot learn from their mistakes, they are likely to commit the same offense again once Internet connection is reestablished. A system that fails to tell users why their behavior is wrong or undesirable is also unlikely to be socially desirable. Such a system is generally perceived to be unfair and illegitimate, and it may undermine the public confidence in not only the copyright system, but the legal system in general.[199] In fact, if the disconnected users believe they have been treated unfairly, upon reconnection they may even commit a bigger offense to exact revenge on what they perceive as an unjust system.

It is important to keep in mind that § 512(i) builds in some discretion for ISPs to determine whether the behavior of repeat infringers should result in heightened punishment. As the provision states, the policy is one "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."[200] By adding the phrase "in appropriate circumstances," Congress anticipates the time when certain actions, such as Internet disconnection, will be deemed inappropriate. One could also argue that a system that does not allow infringers to learn from their mistakes would be inappropriate. As Professor Nimmer reminded us, "[N]ot all subscribers who are repeat infringers must be terminated; it is only when 'appropriate circumstances' are present that termination becomes mandatory."[201]

C. *Reasonable Alternative Access*

The graduated response system needs to take into account the availability of reasonable alternative access for those users whose Internet service is suspended. As noted above, the Internet has become a very important part of everybody's life. Through the use of these technologies, people can now converse with others via e-mail and online chats, look up information in virtual libraries, increase knowledge by taking distance-learning courses, publish social commentaries on their own websites, and develop social communities in the virtual world.

---

198. As Fred von Lohmann has noted, it is important to understand how subscribers will be notified in a graduated response system—for example, "[W[hat if your 'third notice' ends up caught in your spam folder, or your teenager intercepts the letters[]?" Anderson, *supra* note 4 (providing suggestions from Fred von Lohmann of the Electronic Frontier Foundation over areas in the graduated response system that warrant greater scrutiny); *see also* A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy"—Causes and (Partial) Cures*, 67 BROOK. L. REV. 605, 674–78 (2002) (criticizing the ICANN's Uniform Domain Name Dispute Resolution Policy for its failure to ensure that the registrant has received actual notice of the complaint).

199. *See* Yu, *supra* note 31 (manuscript at 35 & n.194).

200. 17 U.S.C. § 512(i) (2006) (emphasis added).

201. 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[D][3].

In addition to entertainment, the Internet can now be used for communications, healthcare, education, career development, commerce, and online banking. In recent years, government has also relied heavily on the Internet to disseminate information and to provide public services, such as voting registration, renewal of license plates, tax filing, and FEMA insurance enrollment.[202] For example, 2010census.gov was prominently displayed in a controversial Super Bowl commercial that cost taxpayers $2.5 million for only thirty seconds.[203]

From the human rights standpoint, maintaining such alterative access is also rather important. In his defense of the graduated response system, Professor Strowel observed: "[T]he French graduated response largely targets Internet access at home. A person will thus be able to use other access points, whether at work, in internet coffee shops, through relatives, or by using devices other than a home computer such as mobile devices with email and browsing capabilities."[204] Such an observation is particularly important in light of Article 10 of the European Convention for Human Rights.[205] Some countries like Estonia, Finland, Greece, and Spain have also mandated universal broadband access[206] or recognized a right to broadband services (even though that right has yet to reach the status of a human right).[207]

Moreover, it is worth comparing the disconnection initiated by the graduated response system against the limited Internet access still enjoyed by prisoners and parolees. For many of these people, including those who have committed Internet and Internet-related crimes,[208] Internet

202. *See, e.g.*, Anderson, *supra* note 4 (noting the observations of Fred von Lohmann of the Electronic Frontier Foundation); Weinberg, *supra* note 28.

203. Dan Chapman & Leon Stafford, *Census Asks Citizens to Help Hold Down Cost of Counting*, ATLANTA J.-CONST., Mar. 9, 2010, at B6; Paul Farhi, *These Are Census Ads? Go Figure*, WASH. POST, Mar. 6, 2010, at C1.

204. Strowel, *supra* note 2, at 83.

205. Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 221.

206. *See* Genan Zilkha, Note, *The RIAA's Troubling Solution to File-Sharing*, 20 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 667, 693 (2010); Saeed Ahmed, *Fast Internet Access Becomes a Legal Right in Finland*, CNN.COM, Oct. 15, 2009, http://edition.cnn.com/2009/TECH/10/15/finland.internet.rights/index.html; *Spain Makes Broadband a Universal Right*, CBC NEWS, Nov. 18, 2009, http://www.cbc.ca/technology/story/2009/11/18/spain-universal-broadband-access.html; Colin Woodard, *Estonia, Where Being Wired Is a Human Right*, CHRISTIAN SCI. MONITOR (Boston, Mass.), July 1, 2003, at 7, http://www.csmonitor.com/2003/0701/p07s01-woeu.html.

207. *See* Bridy, *supra* note 50 (manuscript at 49); Zilkha, *supra* note 206.

208. *See* Habib, *supra* note 106, at 1073–78 (explaining the important distinction between Internet crime and Internet-related crime, or computer crime and computer-related crime). As one author noted:

> [Computer related crimes are those] in which computers are used as tools or targets of the criminal offense, but for which knowledge of the workings of a computer is not essential for the successful commission of the offense. Thus, a chain letter typed on a computer's word processing software and thereafter

disconnection is not the preferred punishment.[209] Nor is disconnection an absolute ban, devoid of built-in discretion from the authorities, such as probation officers.[210] Under most circumstances, the draconian sanction of Internet disconnection is often replaced by monitored access,[211] filtering, site blocking,[212] unannounced manual inspection,[213] or a combination of these options. As the Second Circuit explained in *United States v. Peterson*:

> Computers and Internet access have become virtually indispensable in the modern world of communications and

---

> mailed to victims of a fraudulent solicitation is probably not a computer crime, despite the fact that knowledge of the word processing software facilitated the commission of the offense. A similar chain letter sent out over the Internet, and soliciting electronic funds transfers comes closer to a true computer crime especially if responses are electronically sorted or manipulated.

Mark D. Rasch, *Criminal Law and the Internet*, *in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES 141, 143 (Joseph F. Ruh Jr. ed., 1996).

209. Thus far, there has been "a circuit split over the degree to which courts should restrict a convicted sex offender's access to computers and the Internet." Brant, *supra* note 106, at 781. *Compare* United States v. Peterson, 248 F.3d 79, 82–83 (2d Cir. 2001) ("[T]he broad restrictions on [the convict's] computer ownership and Internet access are not 'reasonably related' to 'the nature and circumstances of the offense' or [the convict's] 'history and characteristics.' . . . We believe the breadth of the restrictions on computer and Internet use made those restrictions excessive." (internal and external citations omitted)), *with* United States v. Paul, 274 F.3d 155, 169 (5th Cir. 2001) (declaring that "the supervised release condition at issue in the instant case is reasonably related to Paul's offense and to the need to prevent recidivism and protect the public"), *and* United States v. Knights, 534 U.S. 112, 119 (2001) ("Inherent in the very nature of probation is that probationers 'do not enjoy 'the absolute liberty to which every citizen is entitled.' Just as other punishments for criminal convictions curtail an offender's freedoms, a court granting probation may impose reasonable conditions that deprive the offender of some freedoms enjoyed by law-abiding citizens." (internal citation omitted)).

210. For example, "The term of supervised release [of a convicted child pornographer] included a special condition directing that Crandon not 'possess, procure, purchase or otherwise obtain access to any form of computer network, bulletin board, Internet, or exchange format involving computers unless specifically approved by the United States Probation Office.'" United States v. Crandon, 173 F.3d 122, 127 (3d Cir. 1999).

211. *See* United States v. Holm, 326 F.3d 872, 877–79 (7th Cir. 2003) ("Various forms of monitored Internet use might provide a middle ground between the need to ensure that Holm never again uses the Worldwide Web for illegal purposes and the need to allow him to function in the modern world.").

212. *See* United States v. White, 244 F.3d 1199, 1206 (10th Cir. 2001) ("To limit [the convict's] use of the Internet to obtain child pornography or other sexually explicit material, filtering software is available to interpose a barrier between the computer's web browser and Internet connection. These programs filter objectionable material either by blacklisting sites and removing them from access, or by whitelisting the sites, blocking access to all sites except those listed on the 'white' list based on categories of content.").

213. *See* United States v. Freeman, 316 F.3d 386, 392 (3d. Cir. 2003) ("There is no need to cut off [the convict's] access to email or benign internet usage when a more focused restriction, limited to pornography sites and images, can be enforced by unannounced inspections of material stored on [his] hard drive or removable disks.").

> information gathering. The fact that a computer with Internet access offers the possibility of abusive use for illegitimate purposes does not, at least in this case, justify so broad a prohibition. . . . Although a defendant might use the telephone to commit fraud, this would not justify a condition of probation that includes an absolute bar on the use of telephones. Nor would defendant's proclivity toward pornography justify a ban on all books, magazines, and newspapers.[214]

Some commentators have also emphasized the Internet's importance for reintegrating convicted offenders into society.[215]

In light of these alternative solutions for those who have been convicted before a court of law, one has to wonder whether Internet disconnection is an excessive and unnecessary sanction for repeat online copyright infringement. In fact, one can easily think of many circumstances when Internet disconnection should be replaced by bandwidth reduction, monitored access, or site, port, or protocol blocking.[216] If Internet access is no longer available to a repeat infringer—through, say, a group boycott of commercial ISPs—it is also fair to question whether, in today's digital age, the protection of human rights would require governments to provide some form of reasonable alternative access in an effort to respect, protect, and

---

214. 248 F.3d 79, 83 (2d Cir. 2001).

215. As one commentator explained:

> Rehabilitation, one of the goals of the prison system, could benefit greatly from allowing inmates Internet access. The Internet is a powerful educational tool. One state has even mandated the use of computers in community correctional centers to promote literacy. As well as being useful in teaching other skills, computer skills themselves may be tremendously valuable for inmates once they have completed their sentences. One of the prison system's ostensible goals is to help inmates become contributing members of society; as technology and time move forward, computer literacy and knowledge of email and the Internet will become indispensable.

Karen J. Hartman, Legislative Review, *Prison Walls and Firewalls: H.B. 2376—Arizona Denies Inmates Access to the Internet*, 32 ARIZ. ST. L.J. 1423, 1434–35 (2000); *see also* Brant, *supra* note 106, at 803–04 ("To facilitate reintegration, other courts have allowed offenders to have access to the Internet for legitimate purposes.").

216. In the *Digital Britain Final Report*, for example, the technological measures that aimed at reducing or preventing online copyright infringement included:

> Blocking (Site, IP, URL), Protocol blocking, Port blocking, Bandwidth capping (capping the speed of a subscriber's Internet connection and/or capping the volume of data traffic which a subscriber can access); Bandwidth shaping (limiting the speed of a subscriber's access to selected protocols/services and/or capping the volume of data to selected protocols/services); Content identification and filtering . . . .

DEP'T FOR CULTURE, MEDIA & SPORT & DEP'T FOR BUS., INNOVATION & SKILLS, DIGITAL BRITAIN FINAL REPORT 111–12 (2009).

fulfill one's free speech rights as well as other Internet-implicated civil liberties.

The issue of alternative access becomes even more important in small cities or rural areas, where there may be only *one* broadband provider.[217] An Internet disconnection, therefore, may mean total disconnection from the Internet. Such disconnection will become a serious hardship, as compared to a mere inconvenience. In fact, it remains disturbing to find industry representatives suggesting that one could change broadband service just like how one applies for a new email account. Unfortunately, in small cities and rural areas, things are quite different from what one would expect in a major city like London, New York, or Paris!

Moreover, the push for Internet disconnection is highly inconsistent with the government's ongoing efforts to bridge the digital divide[218] and strengthen infrastructural development in rural areas.[219] Such a draconian measure also goes against our deep and established commitment to universal service in the area of communications technology.[220] To further complicate matters, some users may have forgone both plain old telephone service and mobile telephony to rely on VOIP (voice over Internet protocol). Because VOIP depends on Internet connection, an Internet disconnection may mean a cutoff of emergency calls, such as the 911 service.[221] If ISPs are required to distinguish between VOIP and other forms of online content to avoid this type of situation, such a requirement would prevent the ISPs from respecting the principle of network neutrality.

---

217. *See* Anderson, *supra* note 4 (noting the suggestion of Fred von Lohmann of the Electronic Frontier Foundation); *cf.* Nate Anderson, *Towards a Kinder, Gentler "Three Strikes" for File-sharers*, ARS TECHNICA, Feb. 1, 2010, http://arstechnica.com/tech-policy/news/2010/02/dropping-car-analogies-and-finding-common-ground-on-copyright.ars (noting the observation of John Robertson, member of the U.K. parliament, that this problem is attributed in a large part to the lack of competition for the "last-mile" in U.S. telecommunications policy).

218. *See generally* Peter K. Yu, *Bridging the Digital Divide: Equality in the Information Age*, 20 CARDOZO ARTS & ENT. L.J. 1 (2002) (providing an overview of the digital divide).

219. *See* Condon, *supra* note 8 (reporting that the recent government stimulus package allocated more than $7 billion for broadband deployment); *see also* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 118, 128 (providing $4.7 billion in the Broadband Technology Opportunities Program to promote and improve access to broadband service in underserved and unserved areas).

220. *See generally* Milton Mueller, *Telecommunications Access in the Age of Electronic Commerce: Toward a Third-Generation Universal Service Policy*, 49 FED. COMM. L.J. 655 (1997) (discussing some of the universal service issues raised by the convergence of card-based commerce and telecommunications access).

221. *See* Alex Curtis, 2010 State of the Net Three Strikes Panel—What MPAA and RIAA Don't Want You to Know, http://www.publicknowledge.org/node/2874 (Jan. 28, 2010); *see also* Nimmer, *supra* note 80, at 205 (noting the problem posed in the situation where "lifeline telephone service is bundled in a given locality with Internet access").

D. *Minimized Collateral Damages*

The policy should not result in collateral damages, such as the tying of Internet access to the availability of TV service, landline or mobile telephone service, or all or some of the above in a so-called "double play," "triple play," or "quadruple play" package.[222] Similarly, and more importantly, the behavior of dependent school-age children should not be used to blackmail their parents into submission.

Individual responsibility is the key feature of the modern criminal law system. A policy that emphasizes collective responsibility is retrograde; it would seriously undermine the progress society has made in the past couple of centuries. Although one could still argue that the parents or other family members may still have access in a workplace, not to mention the fact that parents and guardians have responsibility over their children, it is important not to ignore the fact that many adults now choose to work at home. Many of them either have a home-run business or telecommute to work. A graduated response system, therefore, should take into consideration these potential complications.[223]

E. *Proportionality*

The graduated response system needs to be proportionate.[224] While it is important to protect the interests of copyright holders, it is also important to remember that the protection of copyright interests always has to be balanced against other important societal goals, such as the protection of free speech, free press, and privacy. One may still recall how a senior official from the Department of Homeland Security chastised Sony shortly after its rootkit debacle: "It's very important to remember that it's your intellectual property, it's not your computer."[225]

---

222. *See* Strowel, *supra* note 2, at 83 (defending the French law by pointing out that "in the French scheme, the internet suspension does not (should not) affect the other telecommunications services, for instance the fixed line telephone or the TV service in case of a 'triple play' offer, which would weigh in favor of proportionality").

223. Such complications are likely to pose a significant challenge for policymakers. After all, "the wide availability of internet access through other accounts or devices could mean that the effectiveness of the full graduated response is far from being guaranteed." *Id*.

224. As Professor Nimmer noted in his draft repeat infringer policy, the ISP should

> consider "appropriate circumstances" to remit a strike as including a requirement of proportionality: A subscriber who engages in widescale exploitation, a small percentage of which is determined to constitute copyright infringement (even if willfully so), will not accrue a strike if that infringement appears aberrational in the entire context of the subscriber's exploitation.

Nimmer, *supra* note 80, at 217. Nevertheless, he concedes that proportionality can cut both ways, as a twice-convicted peer-to-peer user may claim that "his infringement amounts to a tiny fraction of all his online (and other) activity." *Id*. at 217–18.

225. Carrie Kirby, *Sony Halts Anti-Piracy Software*, S.F. CHRON., Nov. 12, 2005, at C1.

In the grand scheme of things, copyright protection is unlikely to be considered a very high priority for either law enforcement officials or most law-abiding citizens.[226] If priority is, in fact, needed, law enforcement officials are likely to focus more on commercial piracy and counterfeiting than on individual file sharing. Thus, if the graduated response system is to be convincing and intuitive, it needs to take into consideration the general public expectation of rather limited law enforcement concerning ordinary file-sharers. The more the sanctions correspond to those in other areas of law enforcement, the more people will consider the system legitimate, and the more effective it will be in guiding user behavior.

F. *Flexibility*

The graduated response system needs to be flexible. Copyright law is notoriously complex, subtle, and context-dependent.[227] Except when the infringement involves verbatim copying, such as in file-sharing cases, identifying copyright infringement has proven to be difficult. Indeed, it is not uncommon for courts to spend a considerable amount of time, effort, and resources to determine whether infringement has taken place.[228] As an Australian judge recently noted in *Roadshow Films v. iiNet Ltd.*,[229] a case involving ISP liability:

> [C]opyright infringement is not a straight "yes" or "no" question. The Court has had to examine a very significant quantity of technical and legal detail over dozens of pages in [a legal] judgment in order to determine whether iiNet users, and how often iiNet users, infringe copyright by use of the BitTorrent system.[230]

---

226. *See* Peter K. Yu, *Three Questions That Will Make You Rethink the U.S.-China Intellectual Property Debate*, 7 J. MARSHALL REV. INTEL. PROP. L. 412, 416 (2008) ("Even in the United States[,] . . . the protection of intellectual property rights is generally considered to be of lower priority than the resolution of such domestic problems as the prevention of murders, burglaries, robberies, thefts, arsons, assaults, and distribution of narcotics and child pornography."). *Compare* U.S. DEP'T OF JUSTICE, PROGRESS REPORT OF THE DEPARTMENT OF JUSTICE'S TASK FORCE ON INTELLECTUAL PROPERTY 24 (2006) (stating that 177 defendants were charged with intellectual property offenses in 2004), *with* BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, FEDERAL JUSTICE STATISTICS, http://bjs.ojp.usdoj.gov/fjsrc/var.cfm?ttype=one_variable&agency=AOUSC&db_type=CrimCtCases&saf=IN (select "2004" year, select "Filing offense," and click "PDF" hyperlink) (last visited Oct. 27, 2010) (stating that "criminal cases were commenced against 92,645 defendants" in 2004).

227. *See* Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63, 67–68 (2002).

228. *See* 3 NIMMER & NIMMER, *supra* note 57, § 12B.10[B][2] ("[C]ourts often take many months or years of protracted hearings before they reach a final determination as to whether the challenged conduct amounts to infringement.").

229. (2010) 263 A.L.R. 215 (Austl.).

230. *Id.* ¶ 430.

Moreover, numerous limitations and exceptions exist in copyright law to allow individuals to use copyrighted works without the authorization of copyright holders. Examples of these limitations and exceptions include the originality requirement, the idea-expression dichotomy, durational limits of copyright protection, the fair use privilege, the first sale doctrine, the parody defense, and the *de minimis* use exception.[231]

If Internet disconnection is a potential outcome of repeat online copyright infringement, the limitations, exceptions, and defenses that are available under copyright law need to be built into the graduated response system. To do so, the system needs to provide a mechanism for accused users "to remit a strike."[232] For example, as the third thought experiment has shown, the complexity of fair use analysis and the unsettled nature of this area of the law may make this opportunity particularly important and valuable.[233] In fact, if fair use is needed to provide the oft-mentioned "breathing space" in the copyright system,[234] such breathing space may dictate built-in safeguards within the graduated response system to allow alleged infringers to assert both fair use and the needed defenses.

One could further extend the need to remit strikes to cover other issues in copyright law, such as the lack of originality or invalidity of copyright ownership. As Professor Nimmer explained:

> The problem is not limited to fair use. . . . With different courts reaching different legal determinations about the identical issue applied to the identical work of authorship, the fact that a party loses a copyright case does not always reflect flagrant misconduct. Accordingly, service providers should enjoy wide latitude to remit strikes against parties to infringement suits, even if they ultimately fail to prevail.[235]

---

231. *See* Yu, *supra* note 31 (manuscript at 11).

232. Nimmer, *supra* note 80, at 216. For similar reasons, Professor Bridy argued that, "Users should be given an opportunity to contest notices of infringement with their ISPs as the notices are received and before any sanction is imposed." Bridy, *supra* note 50 (manuscript at 49).

233. *See* Nimmer, *supra* note 80, at 200 ("It hardly seems amiss to remit strikes from parties who advance fair use arguments in objective good faith, even if they fail to win complete judicial vindication.").

234. *See, e.g.*, Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994); *see also* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 578 (2003) (criticizing the DMCA for taking away the "breathing space for thought, exploration, and personal growth" usually protected by the right to privacy); Joseph P. Liu, *Copyright and Breathing Space*, 30 COLUM. J.L. & ARTS 429 (2007) (proposing modifications to existing copyright law that would create breathing space in copyright cases that raise free speech interests); Joseph P. Liu, *Copyright Law's Theory of the Consumer*, 44 B.C. L. REV. 397, 429 (2003) (criticizing the DMCA for its "potential of effectively blocking out some of the breathing space that conventional copyright law made available for more active modes of consumption"); Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1580 (2002) (discussing the "challenge . . . to design legal rules that protect information-rich products against market-destructive cloning while providing enough breathing room for reverse engineering to enable new entrants to compete and innovate in a competitively healthy way").

235. Nimmer, *supra* note 80, at 200.

It is, therefore, no surprise that Professor Nimmer recommended, in his draft repeat infringer policy, that ISPs reserve the right to remit a strike "when the subscriber provides adequate evidence that it infringed unintentionally or in the good faith belief that its conduct did not constitute infringement, or that the adjudicating court considered the issue of infringement to be open to divergent interpretations."[236]

G. *Internet Disconnection as a Last Resort*

The most important of all, Internet disconnection should only be used as *a last resort*. As the House and Senate Reports reasoned in their discussion of § 512(i): "[T]hose who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access."[237] Internet disconnection, therefore, should not be required unless in the most egregious cases.

The fact that a graduated response needs to be introduced does not mean that the system should take the form of a "three strikes" system that suspends the service of Internet users after they have received two warnings from their ISPs about potentially illegal online file-sharing activities. As mentioned earlier, such a draconian sanction can be easily replaced by other less draconian measures, such as bandwidth reduction, monitored access, or site, port, or protocol blocking. Although the scope and length of this Article does not allow me to compare the different measures, it would be, indeed, interesting to compare them to see how each would stack up in relation to each other.[238] In addition, the system can have more than three strikes, especially when the system does not allows users to remit a strike.

Finally, given the potential for ISPs to work together with the copyright holders to develop a shared black list, regulation may be needed to ensure that ISPs in the user's domicile cannot boycott the user as a group, unless government-provided, or perhaps even government-supervised, alternative access is available. While such a group boycott may not rise to the level of an antitrust or competition law violation, it does enlarge the gap created by the unequal bargaining power of Internet users vis-à-vis their ISPs and copyright holders.

CONCLUSION

In the past few years, the entertainment industry has tried many different solutions to address massive online copyright infringement. Many of these solutions, thus far, have ended with very limited success and a

236. *Id*. (italics removed).

237. H.R. REP. NO. 105-551, at 61 (1998); S. REP. NO. 105–90, at 52 (1998).

238. Thanks to Sonia Katyal for making this wonderful suggestion.

considerable amount of collateral damage and unintended side effects. Although the graduated response system seems to provide a good mechanism to combat repeat online copyright infringement, the system does have major shortcomings that will raise significant concerns among civil liberties groups, consumer advocates, and academic commentators.

Based on the foregoing analysis, it is quite clear that it would be ill-advised to institute a graduated response system that targets *alleged* infringers, as opposed to *proven* infringers. Nor does the DMCA or existing copyright law require the adoption of such a system. However, if a graduated response system needs to be introduced to target *proven* infringers, such a system should take into account the seven basic principles outlined in this Article to reduce potential side effects.

There is no easy solution to the copyright challenges brought about by the Internet and new communications technologies. While copyright protection is important, the erosion of due process and the loss of protection of free speech, free press, privacy, and other civil liberties is too high a price for society to pay. In fact, if the existing copyright system cannot provide the needed incentives for authors to create without eroding these other important protections, one has to wonder whether society may be better off completely revamping the copyright system.