Why keep a dog and bark yourself? From intermediary liability to responsibility

Frosio, G. F. (2018). Why keep a dog and bark yourself? From intermediary liability to responsibility. *International Journal of Law and Information Technology*, *26*(1), 1-33. https://doi.org/10.1093/ijlit/eax021

Published in:
International Journal of Law and Information Technology

Document Version:
Peer reviewed version

WHY KEEP A DOG AND BARK YOURSELF? FROM INTERMEDIARY LIABILITY TO RESPONSIBILITY

Giancarlo F. Frosio[*]

26 Oxford Int'l J. of Law and Information Technology (2018)

ABSTRACT

[**1**][**] *This paper contextualizes the recent developments in intermediary liability theory and policy within a broader move towards private ordering online. In this context, online intermediaries' governance would move away from a well-established utilitarian approach and toward a moral approach by rejecting negligence-based intermediary liability arrangements. Miscellaneous policy tools—such as monitoring and filtering obligations, blocking orders, graduated response, payment blockades and follow-the-money strategies, private DNS content regulation, online search manipulation, or administrative enforcement—might reflect this change in perspective. In particular, policy makers—and interested third-parties such as intellectual property rightholders—try to coerce online intermediaries into implementing these policy strategies through voluntary measures and self-regulation, in addition to validly enacted obligations. This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention to police allegedly infringing activities in the Internet. In this sense, the intermediary liability discourse is shifting towards an intermediary responsibility discourse. Further, enforcement would be looking once again for an 'answer to the machine in the machine'. By enlisting online intermediaries as watchdogs, governments would de facto delegate online enforcement to algorithmic tools. Due process and fundamental guarantees get mauled by technological enforcement, curbing fair uses of content online and silencing speech according to the mainstream ethical discourse.*

I. Introduction

Intermediary liability has become one of the most critical Internet governance issues of our time. In particular, modern legal theory—and policy—still struggles

[*] Senior Researcher and Lecturer, Center for International Intellectual Property Studies (CEIPI), Universitè de Strasbourg; Non-Resident Fellow, Stanford Law School, Center for Internet and Society. S.J.D., Duke University School of Law, Durham, North Carolina; LL.M., Duke University School of Law, Durham, North Carolina; LL.M., Strathclyde University, Glasgow, UK; J.D., Università Cattolica del Sacro Cuore, Milan, Italy. The author can be reached at gcfrosio@ceipi.edu. Please note that most materials cited in this paper include an embedded link.

[**] In-text square brackets refer to page numbers in the Version of Record (VoR) publication at Giancarlo Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility' (2018) 26 IJLIT 1-33.

with defining an adequate framework for the liability and responsibility of OSPs for user-generated content. The theoretical—and market—background against which the intermediary liability debate developed has changed considerably [**2**] since the first appearance of online intermediaries almost two decades ago. These changes reflected—or will soon most likely reflect—in changing policy approaches.

As we are entering hyper-history and the fourth revolution, online intermediaries mediate our interaction with ITC and virtual agents in the infosphere.[1] OSPs' role is unprecedented for their capacity to influence the informational environment and users' interactions within it. The ethical implications of OSPs' role in contemporary information societies are raising unprecedented social challenges, as proven by recent examples like the PRISM scandal and the debate on the 'right to be forgotten'. The decisions made by these platforms increasingly shape contemporary life. Whether searching information via Google, discussing trendy topics on Twitter, sharing videos on YouTube, posting pictures on Instagram, making payments via PayPal, or taking employment through Upwork, sophisticated algorithms and company policies enable and constrain our actions. These algorithms take decisions reflecting policy's assumptions and interests that have very significant consequences to society at large, yet there is limited understanding of these processes. Algorithms' accountability remains an issue.[2]

In particular, most creative expression today takes place over communications networks owned by private companies. The decentralized, global nature of the Internet means that almost anyone can present an idea, make an assertion, post a photograph or push to the world numerous other types of content, some of which may be illegal in some jurisdictions or offensive in some cultures.[3] Internet intermediaries play a crucial role in the freedom of expression and communication of

---

[1] See Luciano Floridi, *The Fourth Revolution—How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014) (arguing that after the Copernican, Darwinian, and Freudian Revolutions, humans are once again forced to rethink their role as—after realizing that they were not the centre of the universe, nor of the natural kingdom, and they were not a rational being—they now must interact with virtual entities and agent in a wholly new medium, the infosphere). See also Luciano Floridi, 'Hyperhistory and the Philosophy of Information Policies' (2012) 25 Philosophy and Technology 129, 130 (arguing that "human evolution may be visualised as a three-stage rocket: in prehistory, there are no ICTs; in history, there are ICTs, they record and transmit data, but human societies depend mainly on other kinds of technologies concerning primary resources and energy; and in hyperhistory, there are ICTs, they record, transmit and, above all, process data, and human societies become vitally dependent on them and on information as a fundamental resource").

[2] See Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu, 'Accountable Algorithms' (2017) 165 U Pa L Rev 633; Nicholas Diakopoulos, 'Accountability in Algorithmic Decision Making' (2016) 59(2) Communications of the ACM 56, 56-62; Nicholas Diakopoulos and Michael Koliska, 'Algorithmic Transparency in the News Media' (2016) Digital Journalism.

[3] See Corey Omer, 'Intermediary Liability for Harmful Speech: Lessons from Abroad' (2014) 28 Harvard Journal of Law & Technology 289, 289-323 .

people worldwide. They are subjected to increasing pressure by governments and interest groups which are seeking to control online content by making use of their technical capacities. In practice, that content is increasingly regulated and sometimes censored through private contracts. What should be the role of service providers in moderating the speech they carry for customers, subscribers and others? Should intermediaries have an active role in moderating online speech? Does OSP's role differs from the one of publishers, mass-media, and gate-keepers? Should innocent third parties be enlisted in online enforcement? These are tough questions to answer that have received miscellaneous answers so far even within the same jurisdiction. [**3**]

Apparently, as I argue, the policy discourse is shifting from intermediary liability to intermediary responsibility. Policy approaches might be returning to implement moral theories of intermediary liability, rather than utilitarian or welfare theories. In this case, justification for policy intervention would be based on responsibility for the actions of users as opposed to efficiency or balance innovation vs harm. This is apparent form the enforcement of miscellaneous policy strategies—that will be detailed in the next few pages—and an overall move toward incentivizing intermediaries private ordering online. While private parties' self-awareness of their own duties and obligations might appear a laudable goal to achieve, the demise of a system based on legally enacted obligations and exemptions is not. This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention to police allegedly infringing activities in the Internet. Due process and fundamental guarantees get mauled by technological enforcement, silencing speech according to the mainstream ethical discourse and trampling over the emerging idea of Internet as a fundamental right.[4]

[4] The United States President, Barak Obama declared in a visit to Shanghai that "freedom of access to information is a universal right." Transcript of President Barak Obama's November 16, 2009 Town Hall with Chinese students in Shanghai, as released by the White House (*CBSNews*, 16 November 2016) <http://www.cbsnews.com/news/transcript-obamas-town-hall-in-china>. The Council of Europe has specifically noted, also in response to three-strike legislations proposals, that access to Internet is a "fundamental right." See Monika Ermert, 'Council of Europe: Access to Internet is a Fundamental Right' (*IPWatch*, 8 June 2009); 'Internet Access is a Fundamental Right' (*BBC News*, 8 March 2010) <http://news.bbc.co.uk/2/hi/technology/8548190.stm>. The concept has been stressed by several international and national bodies, such as the UN Human Rights Council, the ITU-UNESCO Commission, the Council of Europe, the Costa Rican Constitutional Court declaring Internet Access essential to the exercise of fundamental rights, or the Finnish government officially making broadband a legal right. See Kaitlin Mara, 'Internet Access And Human Rights Highlighted Alongside UN Human Rights Council' (*IPWatch*, 28 September 2010); Kaitlin Mara, 'ITU-UNESCO Broadband Commission Aims at Global Internet Access' (*IPWatch*, 10 May 2010); 'Acceso a Internet es un derecho fundamental' (*Nacion*, 8 September 2010) <http://www.nacion.com/2010-09-08/ElPais/NotasSecundarias/ElPais2514038.aspx>; 'Finland Makes Broadband a Legal Right' (*BBC News*, 1 July 1, 2010) <http://www.bbc.co.uk/news/ 10461048>. In the civil society debate, the human rights nature of the access to the Internet has been sustained by noting that "the Internet, by facilitating the spreading of knowledge, increases freedom of expression and the value of citizenship." See Marshall Conley and Christina Patterson, *Human Rights and The Internet* (Macmillan 2000). Again, the Internet has been posited as a tool to lower ideological segregation and enhance cultural

II. Intermediary Liability Theoretical Framework

In the mid-nineties, after initial brief hesitation,[5] legislators decided that online intermediaries, both access and hosting providers, had to enjoy exemptions [**4**] for wrongful activities committed by users through their services. The United States introduced these safe harbours first. In 1996, the Communications Decency Act exempted intermediaries from liability for the speech they carry.[6] In 1998, the Digital Millennium Copyright Act introduced specific intermediary liability safe harbours for copyright infringement under more stringent requirements.[7] Shortly thereafter, the eCommerce Directive imposed to Member States the obligation of enacting similar legal arrangements to protect a range of online intermediaries from liability.[8] Other jurisdictions followed suit in more recent times.[9] In most cases, safe harbour legislations provide mere conduit, caching, and hosting exemptions for intermediaries, together with the exclusion of a general obligation on online providers to monitor the information which they transmit or store or actively seek facts or circumstances indicating illegal activity.[10]

Hosting providers are not liable for the information stored, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and—

---

distinctiveness. See Matthew Gentzkow and Jesse M. Shapiro, Ideological Segregation Online and Offline (NBER Working Paper Series No. 15916, April 2010). Contrary views have been sustained by Evgeny Morozov. See Evgeny Morozov, 'The Net Delusion: The Dark Side of Internet Freedom (Public Affairs 2012); Evgeny Morozov, Think Again: The Internet' (*Foreign Policy*, May/June 2010) <http://www.foreignpolicy .com/articles/2010/04/26/think_again_the_internet>.

[5] See Bruce Lehman, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (DIANE Publishing 1995) 114-124 (noting "the best policy is to hold the service provider liable [. . .] Service providers reap rewards for infringing activity. It is difficult to argue that they should not bear the responsibilities."]; see also James Boyle, Intellectual Property? Two Pasts and One Future, Information Influx International Conference, Amsterdam (July 2-4, 2014), <https://www.youtube.com/watch?v=gFDA-G_VqHo>.

[6] See Communications Decency Act of 1996, 47 U.S.C. § 230; *see also* David S. Ardia, 'Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act' (2010) 43 Loyola L Rev 373.

[7] See The Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512 [hereinafter DMCA]

[8] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L 178) 1-16 [hereinafter eCommerce Directive].

[9] See, *e.g.*, Copyright Legislation Amendment Act 2004 (Cth), No. 154, Sch. 1 (Australia); Copyright Modernization Act, SC 2012, c20, § 31.1 (Canada); Judicial Interpretation No. 20 [2012] of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks, December 17, 2012 (China); Federal Law No. 149-FZ, on Information, Information Technologies and Protection of Information, July 27, 2006 (Russia) and Federal Law No. 187-FZ of July 2, 2013 amending Russian Civil Code, § 1253.1.

[10] See, *e.g.*, eCommerce Directive (n 8, at art 12-15; DMCA (n 7, at § 512(c)(1)(A-C)

as regards claims for damages—is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.[11] In particular, the DMCA enacted notice-and-takedown procedures for removing alleged copyright infringing content.[12] Upon righstholders' request, the allegedly infringing materials must be taken down expeditiously by the ISP in order to avoid liability.[13] The removal decision is taken by the private webhosting service and no due process safeguards are in place, except for the counter-notice that the user uploading the material can issue claiming that no infringement has taken place.[14] European jurisdictions, then, impose a higher standard on online intermediaries by providing rightholders with injunctions against intermediaries whose services are used by a third party to infringe a copyright or other intellectual property right.[15] [**5**]

As in the case of the mentioned EU injunctions, bringing pressure to innocent third parties that may enable or encourage violations by others is a well-established strategy to curb infringement. Forcing third parties to act affirmatively to curb infringement would increase the level of compliance to the law. Intermediaries' secondary liability has been based on different theories ranging from moral to utilitarian approaches. A moral approach would argue that encouraging infringement is widely seen as immoral.[16] The second approach is associated with the welfare theory and, more broadly, with the utilitarian approach to law in general. This approach was pioneered thirty years ago by Reiner Kraakman's seminal article, which set the foundations of the so-called "gatekeeper theory" that will be influential

[11] See, *e.g.*, ibid, at art 14; DMCA (n 7, at § 512(c)(1)(A-C),

[12] See DMCA (n 7, at § 512(c)(3), (g)(2-3).

[13] See DMCA (n 7, at § 512(c)(3).

[14] ibid, at § 512(g)(2-3).

[15] See Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10-19 [hereinafter InfoSoc Directive] art 8(3); Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2000 on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 195) 16 [hereinafter Enforcement Directive] art 11.

[16] See Richard Spinello, 'Intellectual Property: Legal and Moral Challenges of Online File Sharing', in Ronald Sandler (ed), *Ethics and Emerging Technologies* (Palgrave Macmillan 2013) 300 (concluding that the behaviour of those that enable P2P sharing by writing and publishing the software that makes it possible is ethically problematic, since it induces and encourages others to act unethically), Mohsen Manesh, 'Immorality of Theft, the Amorality of Infringement' (2006) 2006 Stan Tech L Rev 5 ; Richard Spinello, 'Secondary Liability in the Post Napster Era: Ethical Observations on MGM v. Grokster' (2005) 3(3) J of Information, Communication and Ethics in Society 121; Geraldine Szott Moohr, 'Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory' (2003) 83 B U L Rev 731.

in shaping early online intermediaries' policies.[17] The law would enlist third parties to frustrate or penalize recalcitrant primary infringers, such as bartenders/drunks, accountants/fraudulent clients, employers/illegal immigrants. [18] According to Kraakman,

> [s]uccessful gatekeeping is likely to require (1) serious misconduct that practicable penalties cannot deter; (2) missing or inadequate private gatekeeping incentives; (3) gatekeepers who can and will prevent misconduct reliably, regardless of the preferences and market alternatives of wrongdoers; and (4) gatekeepers whom legal rules can induce to detect misconduct at reasonable cost.[19]

Transposing Kraakman's framework from security regulations—for which it was initially developed—to online infringement, penalties should be imposed on intermediaries in hopes of suppressing infringing behaviours by users only if: otherwise, the incidence of infringement would be unacceptably high, because direct infringers cannot be controlled by socially acceptable sanctions; the intermediaries, on their own, would not intervene to curb infringement—and instead, might foster it; the intermediaries can effectively suppress infringement with minimal capacity for direct infringers to circumvent them; the social and economic cost of penalizing intermediaries are not unacceptably high.[20] This last cost benefit analysis would be [**6**] especially relevant in the case of so called dual-use technologies—technologies that can be used both to infringe others' rights and facilitate social beneficial uses. Lichtman Douglas makes this welfare argument clear by applying it to YouTube:

> [t]he best reason to impose liability on YouTube is that it is in an enormously good position to filter for and in other ways discourage online infringement. The best reason to decline is that there will be some cost associated with filtering, and that cost might discourage future technologists from experimenting with similar products. [. . .]. To the ex-tent that YouTube can discourage infringement at low cost—and it can—copyright law could serve its many competing goals by requiring YouTube to take those steps. By contrast, where the costs of filtering would be crippling or where filtering would in other ways substantially interfere with legitimate amateur video distribution, copyright law could serve those same goals by acknowledging these harms and instead looking for other ways to reward and encourage authors.[21]

---

[17] Reiner Kraakman, 'Gatekeepers: the Anatomy of a Third-Party Enforcement Strategy' (1986) 2(1) Journal of Law, Economics and Organization 53; *see also* C Metoyer-Duran, 'Information gatekeepers' (1993) 28 Annual Review of Information Science and Technology (ARIST) 111.

[18] See Kraakman (n 17) 53.

[19] ibid 61.

[20] See William Fisher, CopyrightX: Lecture 11.1, Supplements to Copyright: Secondary Liability (February 18, 2014), 7:50, <https://www.youtube.com/watch?v=7YGg-VfwK_Y> (applying Kraakman's framework to copyright infringement).

[21] Douglas Lichtman, 'Copyright as Information Policy: Google Book Search from a Law and Economics Perspective' in Josh Lerner & Scott Stern (eds), 9 *Innovation Policy and The Economy* (NBER 2008) 19 (noting that "[t]he best reason to impose liability on YouTube is that it is in an enormously good position to filter for and in other ways discourage online infringement. The best

According to this framework—especially in the copyright infringement domain—judge-made doctrines of secondary liability—including contributory, vicarious and inducement liability—have been developed in the United States in a long line of cases, such as *Sony*,[22] *Fonovisa*,[23] *Napster*,[24] *Aimster*,[25] *Grokster*,[26] and more recently *Vimeo*.[27] Contributory infringement would find its origin in tort law principles—according to which who directly contributes to a tort should be held liable along with the tortfeasor herself—whereas vicarious infringement would be a qualification of the doctrine of *respondiat superior*—a branch of the law of agency that governs responsibility of [**7**] employers for misconduct of their employees.[28] Other countries came up with slightly different doctrines of secondary liability, such the doctrine of authorization in UK and Australia[29] and miscellaneous doctrines

---

reason to decline is that there will be some cost associated with filtering, and that cost might discourage future technologists from experimenting with similar products. [. . .]. To the ex-tent that YouTube can discourage infringement at low cost—and it can—copyright law could serve its many competing goals by requiring YouTube to take those steps. By contrast, where the costs of filtering would be crippling or where filtering would in other ways substantially interfere with legitimate amateur video distribution, copyright law could serve those same goals by acknowledging these harms and instead looking for other ways to reward and encourage authors").

[22] See Sony Corporation of America v Universal City Studios, Inc, 464 US 417 (1984) (holding that a device capable of substantial non-infringing uses does not trigger secondary liability).

[23] See Fonovisa, Inc v Cherry Auction, 76 F3d 259 (9th Cir 1996).

[24] See A&M Records v Napster, 239 F3d 1004 (9th Cir 2001) (finding Napster vicariously liable as it has actual knowledge of infringement and supervisory control).

[25] See In re Aimster Copyright Litigation, 334 F3d 643 (7th Cir 2003) (finding that "willful blindness" constituted knowledge and triggered infringement).

[26] See Metro-Goldwyn-Mayer Studios Inc v Grokster, Ltd, 545 US 913 (2005) (finding that inducement to infringement—evidence of "purposeful, culpable expression and conduct"—triggers liability).

[27] See Capitol Records LLC et al v Vimeo LLC et al, No. 14-1048 (2nd Cir 2016) (finding that video-sharing website Vimeo LLC cannot be held liable for copyright infringement for unknowingly hosting pre-1972 music uploaded by its users and holding that the mere fact that Vimeo employees had viewed videos with copyrighted sound recordings was not enough to prove the company ignored red flags of infringement).

[28] See Reiner Kraakman, 'Vicarious and Corporate Civil Liability' in Michael Faure (ed), *Tort Law and Economics* (Edward Elgar 2009) 134-147; Sverker Högberg, 'The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law' (2006) 107 Col L Rev 909, 915; Alfred Yen, 'Third Party Copyright Liability after Grokster' (2006) 91 Minn L Rev 184**;** Mark Lemley and Anthony Reese, 'Reducing Digital Copyright Infringement without Restricting Innovation' (2004) 56 Stan L Rev 1345, 1366; Charles Wright, 'Actual Versus Legal Control: Reading Vicarious Liability for Copyright Infringement into the Digital Millennium Copyright Act of 1998' (2000) 75 Wash L Rev 1005, 1013.

[29] See CBS Songs Ltd v Amstrad Consumer Electronics Plc [1988] UKHL 15 (finding manufacturer and seller of hi-fi equipment not liable when applying authorization liability of intermediaries facilitating the copyright-infringing actions of their users); Roadshow Films Pty Ltd v iiNet Limited [2012] HCA 16 (High Court of Australia 2012) (holding that iiNet, Australia's second largest ISP,

based on tort law or extra-contractual liability in most civil law countries, ranging from strict liability to negligence or no liability and depicting at times a very confused international panorama.

From Intermediary Liability to Intermediary Responsibility

Apparently, there is a revival of moral approaches to intermediary liability. Legal theory is increasingly shifting the discourse from liability to enhanced 'responsibilities' for intermediaries under the assumption that OSPs' role is unprecedented for their capacity to influence the informational environment and users' interactions within it.[30] Hence, academia, policy-makers and society increasingly ascribe a public role to online intermediaries.[31] According to Shapiro, 'in democratic societies, those who control the access to information have a responsibility to support the public interest. […] these gatekeepers must assume an obligation as trustees of the greater good'.[32] The ethical implications of OSPs' role in contemporary information societies are raising unprecedented social challenges, as proven by recent examples like the PRISM scandal and the debate on the 'right to be forgotten'. The discourse now focuses on moral responsibilities of OSPs in contemporary societies and aims at building ethical frameworks [**8**] for the understanding of OSPs responsibilities, e.g. corporate social responsibilities or

---

was not liable for authorizing its customers' infringement of copyright films downloaded over BitTorrent); Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242 (Federal Court of Australia 2005) (finding Sharman, who operated the Kazaa filesharing platform, liable for authorizing the infringements of its users); University of New South Wales v. Moorhouse [1975] HCA 26 (High Court of Australia 1975) (finding the University of New South Wales liable for authorizing the infringements of those who used the photocopiers it provided in its library). See also Jane Ginsburg and Sam Ricketson, 'Inducers and Authorisers: A Comparison of the US Supreme Court's Grokster Decision and the Australian Federal Court's KaZaa Ruling' (2006) Columbia Public Law and Legal Theory Working Papers 0698/2006.

[30] See eg Communication from the Commission to the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, COM(2017)555final, 28 September 2017, § 6 (noting "the constantly rising influence of online platforms in society, which flows from their role as gatekeepers to content and information, increases their responsibilities towards their users and society at large).

[31] Pressure comes increasingly from users as well as recent lawsuits against platforms supposedly liable of fomenting extremism, radicalism—and related terroristic actions—might prove. See 'Orlando nightclub victims' families sue Twitter, Google, Facebook' (*CNBC*, December 21, 2016) <http://www.cnbc.com/2016/12/21/orlando-nightclub-victims-families-sue-twitter-google-facebook.html>.

[32] Andrew Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know* (Public Affairs 2000) 225.

human rights. Addressing the OSPs' role would require a coordinated interdisciplinary theorizing able to consider legal, social, and ethical standpoints.[33]

This move from intermediary liability to platform responsibility has been occurring first at a theoretical level, with special focus on intermediaries' corporate social responsibilities and their role in implementing and fostering human rights.[34] As made obvious from the literature cited in the next few pages, the term 'responsibility' have been increasingly deployed to address platforms' governance. In the introduction to *The Responsibilities of Online Service Providers*, Mariarosaria Taddeo and Luciano Floridi noted that—given their prominent role of in the present society—online intermediaries are increasingly expected to act according to current social and cultural values, which rises "questions as to what kind of responsibilities OSPs should bear, and which ethical principles should guide their actions'.[35] Taddeo and Floridi argued that service providers lack an ethical framework that can "(a) define [their] responsibilities and (b) provide the fundamental sharable principles necessary to guide OSPs' conduct within the multicultural and international context in which they operate."[36] In search of a model enabling the definition of OSPs responsibilities with the well-being of the informational environment,[37] Taddeo and Floridi distinguish OSP's responsibilities on the basis of the different kinds of information that they control. They identify three important set of ethical problems, the organization and managing of access to information, censorship and freedom of speech, and users' privacy.[38] First, according to the authors, the issue at stake is whether OSPs bear any moral responsibilities for circulating on their infrastructures third-party generated content that may prove harmful, rather than whether OSPs should be held morally responsible for their users' actions.[39] In this respect, some authors argued that it may be desirable to ascribe moral responsibilities to OSPs with respect to the circulation of harmful material.[40] In putting forward a normative

[33] Workshop 'Understanding the Responsibilities of Online Service Providers in Information Societies', Oxford Internet Institute, University of Oxford, UK, 9 October 2015

[34] See Emily B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (CUP 2015); Dennis Broeders et al, 'Does Great Power Come with Great Responsibility? The Need to Talk About Corporate Responsibility' in Mariarosaria Taddeo and Luciano Floridi, The Responsibilities of Online Service Providers (Springer 2017) 315-323.

[35] Mariarosaria Taddeo and Luciano Floridi, 'New Civic Responsibilities for Online Service Providers' in Mariarosaria Taddeo and Luciano Floridi, *The Responsibilities of Online Service Providers* (Springer 2017) 1.

[36] Mariarosaria Taddeo and Luciano Floridi, 'The Debate on the Moral Responsibility of Online Service Providers' (published online November 27, 2015) Sci Eng Ethics 1, 1.

[37] ibid

[38] ibid 5.

[39] ibid 10.

[40] See Vincent Cerf, 'First, Do No Harm' (2011) 24(4) Philosophy & Technology 463, 465 (noting "the opportunity and challenge that lies ahead is how Internet actors will work together not only to do

approach to the responsibility of Internet intermediaries for third-party content they host, Thompson argued that our focus should be on their responsibility towards the [**9**] reasoning processes in reaching decisions, rather than on their outcomes.[41] We should not expect perfection from intermediaries, but responsible efforts like journalists who are entitled to make mistakes, if only they seek responsibly to avoid these.[42]

Again, OSPs responsibilities with respects to Internet freedom and human rights—with emphasis on freedom of speech and information—have emerged as an additional open question. Corporate social responsibility theory have been ported to cyberspace to deploy human rights principles to non-public bodies, which operate largely outside the remit of traditional human rights law.[43] Arguments have been made that obligations pertaining to States—such as those endorsed by the UN Human Rights Council declaration of Internet freedom as a human right[44]—should be extended to online platforms as well.[45] In particular, the preamble of the Universal Declaration of Human Rights appears to support corporate obligations to protect human rights where it mentions that "every individual and every organ of society" should strive to promote these rights.[46] Other international instruments to that effect have been identified in the Declaration of Human Duties and Responsibilities,[47] the

---

no harm, but to increase freedom from harm"); Anton Vedder, 'Accountability of Internet Access and Service Providers—Strict Liability Entering Ethics?' (2001) 3(1) Ethics and Information Technology 67, 67–74; Herman Tavani and Frances Grodzinsky, 'Cyberstalking, Personal Privacy, and Moral Responsibility' (2002) 4(2) Ethics and Information Technology 123, 123–132.

[41] see Marcelo Thompson, 'Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries' (2016) 18 (4) Vand J Ent & Tech L 783, 783-784.

[42] ibid

[43] See Laidlaw (n 34) (noting that ultimately, however, the largely voluntary nature of CSR instruments makes it a problematic candidate as a governance tool for IIGs and freedom of speech).

[44] See Human Rights Council of the United Nations, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet (2012); see also David J. Karp, 'Transnational Corporations in 'Bad States': Human Rights Duties, Legitimate Authority and the Rule of Law in International Political Theory' (2009) 1(01) International Theory 87 (noting that an argument that OSPs are expected to respect human rights is made problematic by the fact that international obligations address states, rather than private parties).

[45] See Florian Wettstein, 'Silence as Complicity: Elements of a Corporate Duty to Speak out Against the Violation of Human Rights' (2012) 22(01) Business Ethics Quarterly 37, 37–61; Stephen Chen, 'Corporate Responsibilities in Internet-Enabled Social Networks' (2009) 90(4) Journal of Business Ethics 523, 523–536 (arguing that social networks bear both moral and legal responsibility to respect human rights because of the centrality of their role). But see George Brenkert, 'Google, Human Rights, and Moral Compromise' (2009) 85(4) Journal of Business Ethics 453, 453–478 (stressing the need to consider the context in which companies act before assessing their moral responsibilities)

[46] See Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), Preamble.

[47] See UNESCO Declaration of Human Duties and Responsibilities (Valencia Declaration) (1998).

preamble of the UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises,[48] and the UN Guiding Principles on Business and Human Rights.[49] Recently, the United Nations Human Rights Council adopted a resolution on the promotion, protection and enjoyment of human rights on the internet, which also addressed a legally binding instrument on corporations' responsibility to ensure human rights.[50]

Finally, copious literature argued that OSPs might have moral responsibility with respects to users' privacy, while being responsible for a devaluation of privacy.[51] [**10**] OSPs and social networks would incentivize users to share more information, exploiting the "privacy paradox"[52] and forms of "privacy myopia."[53] The paradox and myopia lie in the fact that—albeit being aware of the privacy risk involved—individuals continue to surrender their privacy bit by bit by giving away their data too often and too cheaply.[54] OSPs would have the moral responsibility to protect users' privacy by providing users with the maximum level of control over the access to the information that they share.[55] In addition, when it comes to access to personal information by unauthorized parties regardless of the privacy settings set by the individuals, a communitarian and a proxy approach have been proposed. The communitarian approach would shift moral responsibility to control information and

[48] See UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises (August 13, 2003).

[49] See United Nations, Human Rights, Office of the High Commissioner, Guiding Principles on Business Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework (2011) [hereinafter UN GPBHRs].

[50] See United Nations Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/26/13 (20 June 2014).

[51] See Taddeo and Floridi (n 36) 16-18.

[52] See Patricia A. Norberg, Daniel R. Horne & David A. Horne, 'The Privacy Paradox: Personal information Disclosure Intentions versus Behaviors' (2007) 41(1) Journal of Consumer Affairs 100–126 ; see also Man Qi and Denis Edgar-Nevill, 'Social Networking Searching and Privacy Issues' (2011) 16(2) Information Security Technical Report 74, 74.

[53] See Michael Fromkin, 'The Death of Privacy?' (2000)52 Stanford L Rev 1461, 1502-1503.

[54] ibid

[55] See Richard A. Spinello, 'Privacy and Social Networking Technology' (2011) 16 International Review of Information Ethics 12. See also Gordon Hull, Heather Lipford and Celine Latulipe, 'Contextual Gaps: Privacy Issues on Facebook' (2011) 13(4) Ethics and Information Technology 289, 289–302 (also arguing in favour of a proactive approach of OSPs to protect privacy).

protect privacy to the community,[56] while the proxy approach would bring moral responsibility upon OSPs and other intermediaries.[57]

The proxy approach has been increasingly deployed, especially in Europe as the enforcement of the right to be forgotten may prove.[58] This proxy approach would lead to intermediary accountability rather than liability. Shifting the discourse to copyright infringement especially, Martin Husovec argued that the European Union law increasingly forces Internet intermediaries to work for the rightsholders by making them accountable even if they are not tortiously liable for actions of their users.[59] According to Husovec, the shift from liability to accountability has occurred by derailing injunctions from the tracks of the tort law.[60]

Theoretical analysis of corporate social responsibility in cyberspace have been backed up by conspicuous practice. Some projects developed best practices that might be implemented by intermediaries in their terms of service with special emphasis on protecting fundamental rights.[61] For example, under the egis of the [**11**] Internet Governance Forum, the Dynamic Coalition for Platform Responsibility aims to delineate a set of model contractual-provisions.[62] This provisions should be compliant with the UN "Protect, Respect and Remedy" Framework as endorsed by the UN Human Rights Council together with the UN Guiding Principles on Business and Human Rights.[63] Appropriate digital labels should signal the inclusion of these model contractual provisions in the Terms of Service of selected platform providers to "help Internet users to easily identify the platform-providers who are committed to

---

[56] See Kieron O'Hara, 'Intimacy 2.0: Privacy Rights and Privacy Responsibilities on the World Wide Web' in Proceedings of the WebSci10: Extending the Frontiers of Society On-Line, Raleigh, NC, 26-27 April 2010. See also Heng Xu, 'Reframing Privacy 2.0 in Online Social Networks' 14(4) U Penn J of Constitutional L 1077 (2012).

[57] See Jeff Smith, Tamara Dinev and Heng Xu, 'Information Privacy Research: An Interdisciplinary Review' (2011) 35(4) MIS Quarterly 989.

[58] See Taddeo and Floridi (n 36) 18-20.

[59] See Marin Husovec, 'Accountable, Not Liable: Injunctions Against Intermediaries' (2016) TILEC Discussion Paper 2016-012 <http://ssrn.com/abstract=2773768>; Martin Husovec, Accountable, Not Liable: How Injunctions Against Intermediaries Change Intermediary Liability In Europe, Stanford Law School, April 13, 2016, <http://www.husovec.eu/2016/05/accountable-not-liable-video-new-paper.html>; Accountable Not Liable: How Far Should Mandatory Cooperation of Intermediaries Go? <http://accountablenotliable.org>.

[60] ibid

[61] See, *e.g.*, Jamila Venturini, Luiza Louzada, Marilia Maciel Nicolo Zingales, Konstantinos Stylianou Luca Belli, Eduardo Magrani, *Terms of Service and Human Rights: Analysing Contracts of Online Platforms* (CoE, FGV Direito Rio, Editora Revan 2016).

[62] See Dynamic Coalition on Platform Responsibility: a Structural Element of the United Nations Internet Governance Forum <http://platformresponsibility.info>.

[63] See UN GPBHRs (n 49.

securing the respect of human rights in a responsible manner."[64] Again, the Global Network Initiative (GNI) put together a multi-stakeholder group of companies, civil society organizations, investors and academics to create a global framework to protect and advance freedom of expression and privacy in information and communications technologies. The GNI's participants—such as Facebook, Google, LinkedIn, Microsoft and Yahoo—committed to a set of core documents, including the GNI Principles, Implementations Guidelines and Accountability, Policy & Learning Framework.[65] Ranking Digital Rights is an additional initiative that promotes best practices and transparency among online intermediaries.[66] This project ranks Internet and telecommunications companies according to their virtuous behaviour in respecting users' rights, including privacy and freedom of speech. In November 2015, the first project's report ranked 16 companies, in different countries, on 30 different measures.[67] Companies scored between 65 and 13 percent.[68] Most companies received a failing grade for their public commitments and disclosed policies affecting users' freedom of expression and privacy.[69]

However, there are counter-posing forces at work in the present internet governance struggle. A centripetal move towards digital constitutionalism for Internet governance alleviates the effects of the centrifugal platform responsibility discourse. Efforts to draft an "Internet Bill of Rights" can be traced at least as far back as the mid-1990s.[70] Two full decades later, aspirational principles have begun to crystallize into law. Gill, Redeker and Gasser have described more than thirty initiatives spanning from 1999 to 2015 that can be labelled under the umbrella of "digital [**12**] constitutionalism."[71] These initiatives have great differences—and

[64] See Dynamic Coalition on Platform Responsibility (n 62).

[65] See Global Network Initiatives, Principles <http://globalnetworkinitiative.org/principles/index.php>; Global Network Initiatives, Implementation Guidelines <http://globalnetworkinitiative.org/implementation guidelines/index.php>; Global Network Initiatives, Accountability, Policy, and Learning Framework <https://globalnetworkinitiative.org/content/accountability-policy-and-learning-framework>.

[66] See Ranking Digital Rights, https://rankingdigitalrights.org; *see also* Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012).

[67] See Ranking Digital Rights, Corporate Accountability Index, https://rankingdigitalrights.org/index2015.

[68] ibid

[69] ibid

[70] See Lex Gill, Dennis Redeker, and Urs Gasser, Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights (Berkman Center Research Publication No. 2015-15, November 9, 2015).

[71] See Gill, Redeker and Gasser (n 70) 1; *see also* The Internet and Constitutional Law (Oreste Pollicino and Graziella Romeo (eds.), Routledge 2016) (examining the gradual consolidation of a "constitutional core" of internet law at the supranational level and discussing the possibility of the "constitutionalization" of internet law, calling into question the thesis of the so-called anarchic nature of the internet.).

range from advocacy statements to official positions of intergovernmental organizations to proposed legislation—but belong to a broader proto-constitutional discourse seeking to advance a relatively comprehensive set of rights, principles, and governance norms for the Internet.[72]

III. Policy: From Intermediary Liability to Private Ordering

Voluntary and private enforcement of intermediary liability online appears a recent well marked trend that can be explained as a paradigmatic shift from intermediary liability to responsibility. Apparently, this trend is ongoing notwithstanding the negative connotation that private enforcement might have. The 2016 Report of the UN Special Rapporteur for Free Expression has strong language about states pressuring private actors to voluntarily remove content. The Special Rapporteur stressed that in the information and communication technology context, "States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means."[73] Again, the Report recommended that "any demands, requests and other measures to take down digital content or access customer information must be based on *validly enacted law*, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights."[74]

There is, however, a schizophrenic approach to voluntary enforcement to curb allegedly infringing activities online. For example, in a Joint Declaration of the Three Special Rapporteurs for Freedom of Expression, the Rapporteurs encourage the adoption of self-regulatory solutions for the management of rights online, while, at the same time, noting this should be read in conjunction with the importance of minimum safeguards for individual liberties.[75] Again, the OCSE believes that cooperation of intermediaries might be a legitimate tool that shouldn't go too far: "[m]aking private intermediaries more [**13**] transparent and accountable is a legitimate aim to be pursued by participating States through appropriate means.

[72] See Gill, Redeker and Gasser (n 70) 1.

[73] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, November 5, 2016, at § 85.

[74] ibid (emphasis added).

[75] See The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, International Mechanism for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet (2011) 2.b [hereinafter Joint Declaration of the Three Special Rapporteurs for Freedom of Expression].

However, this must not lead to excessive control by public authorities over online content."[76] This schizophrenia might reflect present uncertainty in addressing a complex conundrum, whose policy framework is recently undergoing reconsideration. This cautionary note might explain why—regardless its negative externalities from a fundamental rights perspective—private enforcement has been increasingly put forward as viable policy option—and it is perhaps set to become a standard in Internet governance.

Increasingly, governments—and interested third parties such as intellectual property rightholders—try to coerce online intermediaries into implementing voluntary measures and bear much of the risk of online enforcement. In *Against Jawboning*, Derek Bambauer discusses government pressure on Internet intermediaries that spans a large variety of content types and subject matter.[77] Bambauer cites Representative James Sensenbrenner, pressing U.S. Internet Service Provider Association to adopt putatively voluntary data retention scheme in the following terms: 'if you aren't a good rabbit and don't start eating the carrot, I'm afraid we're all going to be throwing the stick at you'.[78] Either rabbits or dogs, a cost-benefit analysis would most likely suggest online intermediaries to play along. Cost and uncertainty in resisting pressures would be a strong disincentive for online intermediaries. This promotes self-regulatory enforcement strategies and make private ordering a conspicuous trend online.

Public enforcement lacking technical knowledge and resources to address an unprecedented challenge in terms of global human semiotic behaviour would coactively outsource enforcement online to private parties. Enforcement through private ToS moves the adjudication of lawful and unlawful content out of a public oversight. This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention to police allegedly infringing activities in the Internet. Further, enforcement would be looking once again for an "answer to the machine in the machine."[79] By enlisting online intermediaries as watchdogs, governments would *de facto* delegate online enforcement to algorithmic tools—with limited or no accountability.[80] Due process and fundamental guarantees get mauled by technological enforcement, curbing fair uses of content online and silencing speech according to the mainstream ethical discourse.

---

[76] OCSE (n 17) 2.

[77] See also Derek Bambauer, 'Against Jawboning' (2015) 100 Minnesota L Rev 51 (discussing federal and state governments increasing regulation of on-line content through informal enforcement measures, such as threats, at the edge of or outside their authority).

[78] ibid 51-52.

[79] See Charles Clark, 'The Answer to the Machine is in the Machine', in P. Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment*, The Hague: Kluwer Law International, p. 139 (discussing the application of digital right management systems to enforce copyright infringement online).

[80] See Kroll et al (n.

In Europe, the Commission is unenthusiastic about enacting new legislation, which might openly clash with the current liability regime. Coercing intermediaries into "voluntary" measures would have doubtless advantages by allowing to circumvent [**14**] the EU Charter on restrictions to fundamental rights, avoiding the threat of legal challenges, and taking a quicker reform route. According to the *Consultation on Online Intermediaries*, the European Commission's regulatory efforts might emphasize voluntary or proactive measures to remove certain categories of illegal content and allow intermediaries to fulfil enhanced duties of care reasonably expected from them.[81] Further, according to the *Consultation on Modernization of IPRs' Enforcement*, voluntary involvement of intermediaries in enforcing IPRs and cooperation between righstholders and intermediaries should be apparently pushed in European upcoming reforms.[82] Following these Consultations, the *Communication on Online Platforms and the Digital Single Market* puts forward the idea that 'the responsibility of online platforms is a key and cross-cutting issue.' [83] This terminology echoes a discourse that apparently would like to rearrange platform governance from intermediary liability to intermediary responsibility. Again, few months later, in its most recent Communication, the Commission made this goal even clearer by openly pursuing "enhanced responsibility of online platforms" on a voluntary basis. [84] In other words, the Commission would like to impose an obligation on online platforms to behave responsibly by addressing specific problems.[85] Online platforms would be invested by a duty to 'ensure a safe online environment' against illegal activities.[86] Hosting providers—especially platforms—would be called to actively and swiftly remove illegal materials, instead of reacting to complaints. They would be called to adopt effective voluntary '*proactive* measures to detect and remove illegal content online'[87] and are encouraged to do so by using automatic detection and filtering technologies.[88] As the Commission puts it, the goal is 'to engage with platforms in setting up and applying voluntary

[81] See European Commission, Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (September 24, 2015), at 21-23; *see also* eCommerce Directive (n 8, at art 16 (calling on Member States and the Commission to encourage the "drawing up of codes of conduct at Community level by trade, professional and consumer associations or organisations designed to contribute to the proper implementation of articles 5 to 15").

[82] See European Commission, Public Consultation on the Evaluation and Modernisation of the Legal Framework for the Enforcement of Intellectual Property Rights, 9December 2015), at D.1.

[83] Commission, 'Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe' (Communication) COM(2016) 288 Final, 9.

[84] See Commission (30).

[85] See Commission (83) 8.

[86] Communication (30) § 3.

[87] ibid § 3.3.1 (noting that adopting such voluntary proactive measures does not lead the online platform to automatically lose the hosting liability exemption provided by the eCommerce Directive.

[88] ibid § 3.3.2.

cooperation mechanisms aimed at depriving those engaging in commercial infringements of intellectual property rights of the revenue streams emanating from their illegal activities, in line with a 'follow the money' approach'. [89] Again, 'online platforms must be encouraged to take more effective voluntary action to curtail exposure to illegal or harmful content' such as incitement to terrorism, child sexual abuse and hate speech.[90] This should occur, in particular, by setting up a privileged channel with 'trusted flaggers', competent authorities and specialized private entities with specific [**15**] expertise in identifying illegal content,[91] regardless of 'being required to do so on the basis of a court order or administrative decision, especially where a law enforcement authority identifies and informs them of allegedly illegal content'.[92] Online platforms should be able to prevent and contrast online illegal activities by allowing rapid content take-down, setting up proactive intervention, deploying automated filtering technologies, and adopting effective notice and actions mechanisms, which might not necessarily require users to identify themselves when reporting content that thy consider illegal.[93]

Apparently, the Commission aligns its strategy for online platforms to a globalized, ongoing move towards privatization of law enforcement online through algorithmic tools.[94] As EDRi noted private enforcement "downgrades the law to a second-class status, behind the "leading role" of private companies that are being asked to arbitrarily implement their terms of service."[95] Voluntary measures make intermediaries prone to serve governmental purposes under murky, privately-enforced standards, rather than transparent legal obligations. This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention to police allegedly infringing activities in the Internet.

Private ordering and voluntary enforcement is a global trend in recent intermediary liability policy that spans all subject matters relevant to intermediary liability online. Several emerging intermediary liability trends reflect this change in perspective, such as indeed purely voluntary enforcement schemes, including codes of conducts, online search manipulation, follow-the-money strategies, and private DNS content regulation. In addition, there are other enforcement strategies that make more prominent the role of online intermediaries and might be deployed through a

---

[89] See Communication (83) 8.

[90] ibid 9.

[91] Communication (30) § 3.2.1.

[92] ibid § 3.1.

[93] ibid § 3.2.3.

[94] See Joe McNamee, 'Leaked EU Communication – Part 1: Privatized Censorship and Surveillance' (*EDRi*, 27 April 2016) <https://edri.org/leaked-eu-communication-privatised-censorship-and-surveillance>.

[95] 'EDRi and Access Now withdraw from the EU Commission IT Forum discussions' (*EDRi*, 16 May 2016) <https://edri.org/edri-access-now-withdraw-eu-commission-forum-discussions>.

large spectrum of policy options that spans from legally-mandated obligations to private ordering. This is apparently the case of three-strike legislations, filtering obligations, blocking orders dealt almost entirely between intermediaries and righstholders,[96] expanded constructions of the notion of communication to the public to linking and other online activities,[97] and administrative enforcement of intermediary liability online.[98] In the following pages, this paper will [**16**] be describing those trends more tightly connected with the described move from intermediary liability to responsibility, bearing in mind that other policy strategies—as mentioned—might equally signal the same theoretical move but need treatment on their own and are beyond the scope of this paper.

Graduated Response

In the beginning it was 'graduated-response'. So-called 'graduated response' or 'three-strike' regulations—seeking to block out household Internet connections of repeat infringers—do encourage online service providers to exercise policing power on their own over potential infringers. Graduated response arrangements have mostly targeted online copyright infringement through peer-to-peer filesharing.[99] In some

[96] See eg Christophe Geiger and Elena Izyumenko, 'The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking' (2016) American Int'l L Rev 43, 90-96; Husovec (2016) (n 59).

[97] See Case C-160/15 GS Media BV v Sanoma Media Netherlands BV and Others (2016) ECLI:EU:C:2016:644.

[98] See eg AGCOM Regulations regarding Online Copyright Enforcement, 680/13/CONS, 12 December 2013 (Italy) (providing AGCOM with administrative power to enforce online copyright infringement); Giancarlo Frosio, 'Italian Communication Authority Approves Administrative Enforcement of Online Copyright Infringement' (*CISBlog*, 17 December 2013) <https://cyberlaw.stanford.edu/blog/2013/12/italian-communication-authority-approves-administrative-enforcement-online-copyright> (providing an English summary of the AGCOM Regulation); Royal Legislative Decree No. 1/1996, enacting the consolidated text of the Copyright Act, 12 April 1996 (as amended by the Law No. 21/2014, 4 November 2014) (Spain) (creating an administrative body—the Second Section of the Copyright Commission (CPI)—which orders injunctions against information society services who infringe on copyright); Omnibus Bill No 524 (first introduced on June 26, 2013), amending provisions in various laws and decrees including Law No 5651 'Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications', Law No 5809 'Electronic Communications Law' and others (Turkey) (empowering the Presidency of Telecommunications and Communications with broad administrative enforcement prerogatives online); Federal Law No. 139-FZ, on the Protection of Children from Information Harmful to Their Health and Development and Other Legislative Acts of the Russian Federation (aka "Blacklist law"), 28 July 2012 (putting the Roskomnadzor in charge of the Registry and site blocking enforcement); Act on the Establishment and Operation of Korea Communications Commission (KCCA) last amended by Act No. 11711, 23 March 2013 (establishing the KCCA implementing deletion or blocking orders according to the request and standards of the Korea Communications Standards Commission (KCSC), also instituted by the same law).

[99] See Maria Mercedes Frabboni, 'File Sharing and the Role of Intermediaries in the Marketplace: National, European Union and International Developments' in Irini A. Stamatoudi (ed), *Copyright Enforcement and the Internet* (Wolters Kluwer 2010).

instances, graduate response arrangements have been judicially or legislatively mandated. Often, they result from voluntary arrangements. Although little is known regarding the specifics of these agreements, rightsholders might attempt to leverage their content and would only license if the providers implemented a disconnection strategy.

French Hadopi Law or the South Korean Copyright Law have mandated gradual response schemes, actually managed by administrative agencies, rather than intermediaries. French law empowers the HADOPI administrative authority to send warnings to identified infringers and transfer the case to the court in cases of repeat infringement.[100] When the same account is identified for a third time within a period of one year, HADOPI may escalate the case by referring it to the criminal court, where a judge might order a range of penalties, including a 30-day account suspension.[101] In 2009 the South Koren Copyright Act introduced a three-strike regime, [**17**] where a subscriber, or an online bulletin board, which received more than three warnings, is subject to suspension of its account up to six months.[102] The suspension orders to OSPs are made by the Minister of Culture, Sports and tourism, which is an administrative agency.[103] Intermediaries failing to abide to the order will be imposed of a civil fine not exceeding 10 million won.[104] These mechanisms have been implemented in a number of other countries such as New Zealand, Taiwan, and the United Kingdom.[105]

In some instances, court have review the legality of graduated response schemes and issued injunctions mandating arrangements supposedly minimizing negative effects on authors rights. An ISP-administered graduated response scheme has been rejected by Australian courts. The High Court of Australia held that iiNet, Australia's second largest ISP, was not liable for authorising its customers'

---

[100] See Law No. 2009-669 of June 12, 2009, Promoting The Dissemination and Protection Of Creative Works on The Internet (a.k.a. HADOPI law) (France) (providing injunctive measures against any person likely to remedy copyright infringement); Law No. 2009-1311 of October 28, 2009, on the Criminal Protection of Literary and artistic Property on the Internet art 7 and 10 (France) (providing internet suspension sanctions for persons using the Internet to commit infringement and obligations for owner of internet access to secure their internet access).

[101] ibid

[102] See Copyright Act, last amended by Act No. 12137 (30 December 2013) art 133-2 and 133-3 (South Korea).

[103] ibid

[104] ibid

[105] See Copyright (Infringing File Sharing) Regulations 2011 (New Zealand); Copyright Act as amended on 22 January 2014 art 90-4(2) (Taiwan); Digital Economy Act 2010 C. 24 (however, the 'obligations to limit Internet access' have not been implemented yet). See also Anne Barron, 'Graduated response' à l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010' (2011) 3(2) Journal of Media Law 305, 305-347.

infringement of copyright films downloaded over BitTorrent.[106] In contrast, a recent Irish case does exemplify the possible judicial constructions of graduated response schemes in light of users' rights.[107] Sony, Universal and Warner Music, sought an injunction to impose upon UPC Communications, the second largest Irish Internet access provider, an obligation to implement a "Graduated Response Strategy" (GRS) against UPC's subscribers allegedly infringing plaintiffs' copyrights online.[108] According to the injunction finally granted by the court, the GRS cannot encompass any suspension or termination of users' accounts but only the disclosure of information to make a *Norwich Pharmacal* order to finally seek an accounts' suspension or termination.[109] The Court noted, on the issue of allocation of costs, that "because the defendant is the company which profits—albeit indirectly—because it derives revenue from its subscribers who are engaged in this practice, it is the defendant who should, in my view, be primarily liable for the costs." Therefore, according to the Court, UPC should be required to contribute 80% of the costs.[110]

Industry-led self-regulation makes up the largest part of graduated response schemes. In a Memorandum of Understanding between the five largest US broadband ISPs and the entertainment industry, the ISPs agreed on voluntary DMCA-plus measures consisting in the implementation of a 'six strikes' graduate response [**18**] protocol for curbing unauthorized p2p file sharing.[111] However, the Copyright Alert System (CAS) was discontinued in January 2017.[112] CAS set up a cooperative, multi-stakeholder approach in which information service providers served as a watchdog of the rightsholders.[113] CAS would implement a system of multiple alerts, whose conclusive step encompassed the capacity of "your ISP [to]

---

[106] See *Roadshow Films Pty Ltd v iiNet Limited* [2012] HCA 16. See also Nicolas Suzor and B Fitzgerald, 'The Legitimacy of Graduated Response Schemes in Copyright Law' (2011) 34 U New South Wales J L 1.

[107] See *Sony Music & Ors v UPC Communications* [2015] IECH 317. See also Gerard Kelly, 'A Court-Ordered Graduated Response System in Ireland: the Beginning of the End?' (2016) 11(3) Journal of Intellectual Property Law & Practice 183, 183-198.

[108] ibid § 1-8.

[109] ibid § 198, 232-241.

[110] ibid § 247-265.

[111] See Annemarie Bridy, 'Copyright's Digital Deputies: DMCA-plus Enforcement by Internet Intermediaries' in John A. Rothchild (ed), *Research Handbook on Electronic Commerce Law* (Edward Elgar Publishing 2016) 191-195. See also Annemarie Bridy, 'Graduated Response American Style: 'Six Strikes' Measured Against Five Norms' (2012) 23(1) Fordham Intell Prop Media & Ent L J 1, 1-66; Peter K. Yu, 'The Graduated Response' (2010) 62 Fla L Rev 1373.

[112] David Kravets, 'RIP, "Six Strikes" Copyright Alert System' (*ArsTechnica*, 30 January 2017)

[113] See Jill Lesser, 'Copyright Alert System Set to Begin' (*Center for Copyright Information*, 25 February 2013) <http://www.copyrightinformation.org/uncategorized/copyright-alert-system-set-to-begin>.

undertake measures that will temporarily affect your Internet experience."[114] After a fifth alert, ISPs were allowed to take "mitigation measures" to prevent future infringement.[115] If the ISP did not institute a mitigation measure following the fifth alert, it had to enact one after the sixth alert.[116] Mitigation measures included 'temporary reductions of Internet speeds, temporary downgrade in Internet service tier or redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responds to some educational information about copyright, or other measures (as specified in published policies) that the ISP may deem necessary to help resolve the matter'.[117]

Similar multi-stakeholders' agreements have been discussed or implemented also elsewhere. In Australia, an industry-negotiated graduated response Code was submitted to the Australian Communications and Media Authority (ACMA) for registration as an industry code under the Telecommunications Act 1997 (Cth) on 8 April 2015.[118] The Code introduces a Copyright Notice Scheme that requires Internet Service Providers to pass on warnings to residential fixed account holders who are alleged to have infringed copyright.[119] The scheme consists of an escalating series of infringements notices.[120]

In Europe, Ireland—as also seen earlier—has been especially active in implementing graduated response schemes. Eircom was one of the first European ISPs to [**19**] implement a voluntary a Graduated Response Protocol under which Eircom would issue copyright infringement notices to customer, after a settlement had been reached between record companies and Eircom.[121] The Irish Supreme Court later upheld the validity of the scheme.[122] The Data Protection Commissioner believed that this Protocol breached EU and Irish data protection law and issued an enforcement notice requiring Eircom to cease its operation of the Protocol.[123] The

[114] Center for Copyright Information, The Copyright Alert System, What is a Copyright Alert?, http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert.

[115] See Center for Copyright Information, Copyright Alert System (CAS) <http://web.archive.org/web/20130113051248/http://www.copyrightinformation.org/alerts>.

[116] ibid

[117] See Center for Copyright Information (n 114).

[118] See Communications Alliance Ltd, C653:2015 – Copyright Notice Scheme Industry Code (April 2015) <http://www.commsalliance.com.au/__data/assets/pdf_file/0005/48551/C653-Copyright-Notice-Scheme-Industry-Code-FINAL.pdf>.

[119] ibid

[120] ibid

[121] See EIR, Legal Music - Frequently Asked Questions <www.eir.ie/notification/legalmusic/faqs>.

[122] See *EMI v Data Protection Commissioner* [2013] IESC 34.

[123] ibid

Supreme Court found that the enforcement notice was invalid because of the absence of reasons.[124]

Recently, an agreement has been negotiated between major British ISPs and rights-holders—with the support of the UK Government—under the name of Creative Content UK.[125] This voluntary copyright scheme might serve as a work-around of the Digital Economy Act, which have not yet been fully brought into force. According to earlier reports, this scheme might resemble closely the US CAS model with four-strikes, rather than six.[126] It would implement four notices or alerts sent by the ISPs to their subscribers based on IP addresses supplied by the rights-holders, where the IP address is alleged to have been used to transmit infringing content.[127] The notices will be educational only, and there will be no sanction to follow if user behaviour doesn't change.[128]

Graduated response mechanisms have been broadly questioned for their negative implications on users' rights.[129] Other empirical studies highlighted only reductions in illegal downloading, which have been quickly replaced by other form of online piracy, such as online streaming, cyberlockers, sharp increase in VPNs' usage. [130] Arnold et al's 'econometric results indicate that the Hadopi [three strikes] law has not deterred individuals from engaging in digital piracy and that it did not reduce the

---

[124] ibid

[125] Creative Content UK <http://www.creativecontentuk.org>.

[126] See Monica Horten, 'UK ISPs & Music Industry Broker 4-Strikes Copyright Anti-Piracy Deal' ((*IPTegrity*, 9 May 2014) <http://www.iptegrity.com/index.php/digital-britain/964-uk-isps-a-music-industry-broker-4-strikes-copyright-anti-piracy-deal>; Mark Jackson, UK ISPs Agree Voluntary Internet Piracy Warning Letters Scheme (*ISPreview*, 19 July 2014) <http://www.ispreview.co.uk/index.php/2014/07/big-uk-isps-agree-voluntary-internet-piracy-warning-letters-scheme.html>.

[127] ibid

[128] ibid

[129] See, Christophe Geiger, 'Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach' in Paul Torremans (ed), *Research Handbook on the Cross-Border Enforcement of Intellectual Property* (Edward Elgar, 2014) 704; Christopher M. Swartout, 'Toward a Regulatory Model of Internet Intermediary Liability: File-Sharing and Copyright Enforcement' (2011) 31 Northwestern J Int'l L & Bus 499 (concluding that most of the existing proposals intended for graduated response laws deemed to have problems); Alain Strowel, 'The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringements?' in Irini A. Stamatoudi (ed), *Copyright Enforcement and the Internet* 147-159 (Wolters Kluwer 2010); Valérie-Laure Benabou, 'The Chase: The French Insight into the 'Three Strikes' System' in Irini A. Stamatoudi (ed), *Copyright Enforcement and the Internet* (Wolters Kluwer 2010)163-179; Pierre Sirinelli, 'The Graduated Response and the Role of Intermediaries: Avoiding the Apocalypse or a Return to the Sources?' in Lionel Bently, Uma Suthersanen and Paul Torremans (eds), *Global Copyright: Three Hundred Years Since the Statute of Anne, from 1709 to Cyberspace* (Edward Elgar 2010) 478-491

[130] See Rebecca Giblin, 'Evaluating Graduated Response' (2014) 37 Col J L & arts 147.

[**20**] intensity of illegal activity of those who did engage in piracy'.[131] In contrast, graduated response scheme's negative externalities—both in terms of economic and social costs—have been substantial. Due to their lack of effectiveness, graduated response strategies have lost much of their original appeal and have been apparently sidelined as a policy response to online content infringement and speech-related crimes. Much more effective enforcement tools have been implemented or are under discussion.

Proactive Monitoring and Algorithmic Enforcement

Filtering and proactive monitoring have been increasingly sought—and deployed—as enforcement strategy online. Traditionally, online service providers have enjoyed an exemption to any general obligation to monitor the information which they transmit or store or actively seek facts or circumstances indicating illegal activity.[132] The principle of no-monitoring obligations that enforces a knowledge-and-take-down corollary principle does characterize the intermediary liability system as a negligence-based system. This fundamental tenet of online intermediaries' governance has been increasingly challenged.[133] The emergence of proactive monitoring obligations—and the automated or algorithmic enforcement that brings about—would further empower private ordering and enforcement.[134] Proactive monitoring comes first—and largely—as a private ordering approach following rightholders and government pressures to purge the Internet from allegedly infringing content or illegal speech. In the mist of major lawsuits launched against them,[135] YouTube and Vimeo felt compelled to implement filtering mechanisms on their platforms on a voluntary basis. Google lunched Contend ID in 2008.[136] Vimeo

[131] See Michael Arnold, Eric Darmony, Sylvain Dejeanz and Thierry Penard, 'Graduated Response Policy and the Behavior of Digital Pirates: Evidence from the French Three-strike (Hadopi) Law' (28 May 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2380522>. But see Brett Danaher, Michael D. Smith, Rahul Telang, and Siwen Chen, 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France' (2014) 62 The J of Industrial Economics 541, 541-553 (suggesting that suggest that increased consumer awareness of HADOPI caused iTunes song and album sales to increase by 22.5% and 25% respectively relative to changes in the control group).

[132] See eg eCommerce Directive (n 8) art 12-15; DMCA (n 7) § 512(c)(1)(A-C)

[133] See Giancarlo Frosio, 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe' (2017) 12 Oxford J Intell Prop L & Pract (forthcoming), 5-9 (discussing a move from a negligence-based to a strict liability approach in recent proposals);

[134] See eg Sophie Stalla-Bourdillon, 'Internet Intermediaries as Responsible Actors? Why It is Time to Rethink the e-Commerce Directive as Well' in Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2016) 275-293.

[135] See Viacom Int'l v. YouTube Inc 676 F3d 19 (2nd Cir 2012); Capitol Records (n 27); Capitol Records LLC v. Vimeo 972 F Supp 2d 500 (SDNY 2013) (denying in part Vimeo's motion for summary judgment)

[136] YouTube, How Content ID Works <https://support.google.com/youtube/answer/2797370?hl=en>.

adopted Copyright Match in 2014.[137] Both technologies rely on digital fingerprinting to match an uploaded file against a database of protected works provided by rightholders.[138] [**21**]

Proactive monitoring—and filtering—sits on top of the rightsholders' wish list both in the United States and Europe.[139] The promotion of automated filtering emerges as a primary goal on the EU Commission agenda, both on a mandatory and voluntary basis. According to the recent Communication "Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms," hosting providers would be called to adopt effective voluntary "proactive measures to detect and remove illegal content online"[140] and are encouraged to do so by using automatic detection and filtering technologies.[141] In addition, legislatively mandated proactive monitoring obligations to curb online copyright infringement might soon follow in the footsteps of the voluntary measures already adopted by major platforms. In particular, a recent proposal included in the *Copyright in the Digital Single Market Draft Directive* would impose on intermediaries the implementation of effective content recognition technologies to prevent the availability of infringing content.[142] The proposal specifically refers to technologies such as YouTube's Content ID or other automatic infringement assessment systems.[143] Apparently, the proposal would force hosting providers to develop and deploy filtering systems, therefore *de facto* monitoring their networks.

Proactive monitoring and filtering obligations would also find their way in European policy through an update of the audio-visual media legislation. As part of

---

[137] See Chris Welch, 'Vimeo Rolls Out Copyright Match to Find and Remove Illegal Videos' (*The Verge*, 21 May 2014) <https://www.theverge.com/2014/5/21/5738584/vimeo-copyright-match-finds-and-removes-illegal-videos>.

[138] YouTube (n 136).

[139] See Joint Supplemental Comments of American Federation of Musicians et al to U.S. Copyright Office, In the Matter of Section 512 Study: Notice and Request for Public Comment, Docket No 2015-7 (28 February 2017) (the Recording Industry Association of America and 14 other groups calling for stronger regulations that would require internet service providers to block pirated content). See also Amar Toor, 'The RIAA Wants Internet Companies to Begin Filtering Pirated Content' (*The Verge*, February 28, 2017) <http://www.theverge.com/2017/2/28/14760538/riaa-piracy-dmca-filter-copyright-isp>.

[140] Communication (n 30) § 3.3.1 (noting that adopting such voluntary proactive measures does not lead the online platform to automatically lose the hosting liability exemption provided by the eCommerce Directive).

[141] ibid § 3.3.2.

[142] See Commission, 'Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market' COM(2016) 593 final (14 September 2016) art 13. See also Giancarlo Frosio, Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (2017) 111 Northwestern U L Rev Online (forthcoming); Giancarlo Frosio and Christophe Geiger, 'Reaction of CEIPI to the European Commission's Proposal on Certain Uses of Protected Content by Online Services' (2017) CEIPI Research Paper Series (forthcoming).

[143] ibid

its legislative intervention package, the Commission will tackle the proliferation on online video sharing platforms of content that is harmful to minors and of hate speech with its proposal for an updated Audio-visual Media Services Directive.[144] Video hosts can be regulated like broadcasters if they step outside of their passive hosting role by organizing hosted content. The AVMS draft directive lists new obligations to remove and possibly monitor for hate speech. This specific-sector regulation would ask platforms to put in place measures to protect minors from harmful content and to protect everyone from incitement to hatred.[145] Apparently, the [**22**] AVMS revision might erode the eCommerce directive no monitoring obligations for video platforms by asking Member States to "ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to violence or hatred'.[146]

These proposals, however, confirm a well-established trend in recent intermediary liability policy that already emerged at the national level in multiple judicial decisions. Recent case law has imposed proactive monitor obligations on intermediaries for copyright infringement in multiple jurisdictions.[147] Actually, the emerging enforcement of proactive monitoring obligations have been spanning the entire spectrum of intermediary liability subject matters: intellectual property, privacy, defamation, and hate/dangerous speech.[148] In this context, however, notable

---

[144] See Commission, Proposal for a Council Directive amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final.

[145] ibid art 6 and 28.

[146] See Proposal for a Directive of the European Parliament and the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final (25 May 2016) art 6.

[147] APC et al v Google, Microsoft, Yahoo!, Bouygues et Al (TGI Paris 2013) (France) (imposing on search engines an obligation to proactively expunge their search results from any link to the illegal movie streaming website Allostreaming and affiliated enterprises); Google Brazil v Dafra, Special Appeal 1306157/SP (Superior Court of Justice, 24 March 2014) (Brazil) (imposing on YouTube a proactive monitoring obligation and a strict liability standard for infringement of Dafra's copyright in a commercial dubbed by an anonymous user with comments tarnishing Dafra's reputation); GEMA v RapidShare I ZR 80/12 (Bundesgerichtshof, August 15, 2013) (Germany) (finding that—under the TMA—host providers are already ineligible for the liability privilege if their business model is mainly based on copyright infringement); Zhong Qin Wen v Baidu, 2014 Gao Min Zhong Zi 2045 (Beijing Higher People's Court 2014) (finding that it was reasonable for Baidu to exercise a duty to monitor and examine the legal status of an uploaded work once it has been viewed or downloaded more than a certain times).

[148] See Google v Mosley (TGI Paris, 6 November 2013) (France); Max Mosley v Google Inc., 324 O 264/11 (Hamburg District Court, 24 January 2014); Mosley v Google [2015] EWHC 59 (QB) (United Kingdom) (courts in France, Germany, and the UK imposing proactive monitoring obligations to search engines, which were ordered to expunge the Internet from pictures infringing the privacy rights of Max Mosley—former president of Formula 1—caught on camera to have sex with prostitutes

exceptions—such as the landmark Belen case in Argentina—highlight also a fragmented international response to intermediary liability.[149]

As stated by multiple authority,[150] general filtering and monitoring obligations would be inconsistent with the Charter of Fundamental Rights of the European [**23**] Union.[151] In the SABAM cases, the Court explained that filtering measures—and monitoring obligations—would fail to strike a 'fair balance' between copyright and other fundamental rights.[152] In particular, they would undermine users' freedom of expression.[153] Users' freedom to receive and impart information would be struck by the proposal. Automatic infringement assessment systems might undermine the enjoyment of users' exceptions and limitations.[154] DRM effects on exceptions and

---

wearing Nazi paraphernalia); Rolex v. eBay (a.k.a. *Internetversteigerung* II), I ZR 35/04 (BGH, 19 April 2007) (Germany); Rolex v. Ricardo (a.k.a. *Internetversteigerung* III), Case I ZR 73/05, (BGH, 30 April 2008) (Germany) (in the so-called Internet Auction cases I-III, the German Federal Court of Justice—*Bundesgerichtshof*—repeatedly decided that notified trade mark infringements oblige internet auction platforms such as eBay to investigate future offerings—manually or through software filters—in order to avoid trade mark infringement); Delfi AS v Estonia No 64569/09 (ECtHR, 16 June 2015) finding compliant with ECHR a decision imposing monitoring obligation on a news web portal for defamatory users' comments).

[149] See Rodriguez M. Belen v. Google, R.522.XLIX. (Supreme Court, October 29, 2014) (Argentina) (ejecting filtering obligations to prevent infringing links from appearing in search engines' results in the future in a case brought by a well-known public figure for violation of her copyright, honour and privacy).

[150] See C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85 (CJEU) See also Angelopoulos (2017) (n 56) 38-40; Stefan Kulk and Frederik J. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 Europ. Intell. Prop. Rev. 791, 791-794; Darren Meale, '(Case Comment) SABAM v Scarlet: Of Course Blanket Filtering of the Internet is Unlawful, But This Isn't the End of the Story' (2012) 37 Europ. Intell. Prop. Rev. 429, 432; Andrea Montanari, 'Prime Impressioni sul Caso SABAM c. Netlog NV: gli Internet Service Provider e la Tutela del Diritto D'autore Online' (2012) 26(4) Diritto del Commercio Internazionale 1082 ; Evangelia Psychogiopoulou, '(Case Comment) Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers After Scarlet' (2012) 38 Europ. Intell. Prop. Rev. 552, 555.

[151] See Charter of Fundamental Rights of the European Union, C326/391 (26 October 2012) [hereinafter EU Charter].

[152] See Netlog (n 150) § 55.

[153] See EU Charter (n 151) art 8 and 11.

[154] See Leron Solomon, 'Fair Users or Content Abusers? The Automatic Flagging of Non-Infringing Videos by Content ID on Youtube' (2015) 44 Hofstra L. Rev. 237; Corinne Hui Yun Tan, 'Lawrence Lessig v Liberation Music Pty Ltd - YouTube's Hand (or Bots) in the Over-zealous Enforcement of Copyright' 36(6) (2014) EIPR 347, 347-351; Justyna Zygmunt, To Teach a Machine a Sense of art – Problems with Automated Methods of Fighting Copyright Infringements on the Example of YouTube Content ID, Machine Ethics and Machine Law E-Proceedings, Jagiellonin University, Cracow, Poland, November 18-19, 2016, pp. 55-56; Zoe Carpou, 'Robots, Pirates, and the Rise of the Automated Takedown Regime: Using the DMCA to Fight Piracy and Protect End-Users' (2016) 39 Colum J L & Arts 551, 564-582 .

limitations have been highlighted by copious literature.[155] Similar conclusions apply to this scenario. Automated systems cannot replace human judgment that should flag a certain use as fair—or falling within the scope of an exception or limitation. Also, complexities regarding the public domain status of certain works might escape the discerning capacity of content recognition technologies. At the present level of technological sophistication, false positives might cause relevant chilling effects and negatively impact users' fundamental right to freedom of expression. In the own word of the European Court of Justice, these measures

> could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned.[156]

[**24**] Similar points have been highlighted by miscellaneous scholarship. Enforcing online behaviour through automated or algorithmic filtering and fair use does end up inherently in a bad trade-off for fundamental and users' rights. Julie Cohen and Dan Burk argued that fair use cannot be programmed into an algorithm, so that institutional infrastructures will always be required instead.[157] Although changes in technology move fast and unpredictably, the assumption that, since fair use is at heart an equitable doctrine, judgment is not programmable might remain valid. Indeed, the capacity of neural networks to develop more accurate models of many phenomena—maybe even some or most fair uses—is changing the conception of how machines can assess these phenomena.

In general, it was noted that "the design of copyright enforcement robots encodes a series of policy choices made by platforms and rightsholders and, as a result, subjects online speech and cultural participation to a new layer of private ordering and private control."[158] According to Matthew Sag, automatic copyright filtering systems—upon which private agreements between rightholders and online platforms

---

[155] See Giancarlo F. Frosio, *COMMUNIA Final Report on the Digital Public Domain* (report prepared for the European Commission on behalf of the COMMUNIA Network and the NEXA Center) (2011), 99-103, 135-141 <http://www.communia-project.eu/final-report> (discussing most of the relevant literature and major threats that technological protection measures pose for fair dealings, privileged and fair uses).

[156] Netlog (n 150) § 50.

[157] See Dan L. Burk and Cohen, Julie E., 'Fair Use Infrastructure for Copyright Management Systems' (2000) Georgetown Public Law Research Paper 239731/2000 <https://ssrn.com/abstract=239731>.

[158] See Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (2017) 93 Notre Dame L Rev, at 1.

are predicated—"not only return platforms to their gatekeeping role, but encode that role in algorithms and software."[159] In turn, automatic filtering supersedes the safe harbour system and fair use only nominally applies online.[160] In practice, private agreements and automatic filtering determine online behaviour far more "than whether that conduct is, or is not, substantively in compliance with copyright law."[161]

Codes of Conduct, Filtering and Extremism

According to the European Commission, coordinated EU-wide self-regulatory efforts by online platforms should immediately be directed to fight hate speech,[162] incitement to terrorism and prevent cyber-bullying.[163] As an immediate result of this new policy trend, the Commission recently agreed with all major online hosting providers—including Facebook, Twitter, YouTube and Microsoft—on a code of conduct that includes a series of commitments to combat the spread of illegal hate [**25**] speech online in Europe.[164] This includes commitments about faster notice and takedown for illegal hate speech that will be removed within 24 hours and to special channels for government and NGOs notice to remove illegal content.[165]

In partial response to this increased pressure from the EU regarding the role of intermediaries in the fight against online terrorism, major tech companies—Facebook, Microsoft, Twitter and YouTube—announced that they will begin sharing hashes of apparent terrorist propaganda.[166] For some time, You Tube and Facebook

[159] ibid 1.

[160] ibid

[161] ibid

[162] See, for an overview of European law and jurisprudence on incitement to hatred online, Michael Whine, 'European Law on Incitement to Hatred on the Internet' (August 2014).

[163] See Communication (n 83) at 10. Several other documents coming out of the EU on anti-radicalization and countering extremism, including the UK Counter Extremism Strategy and the EU Parliament's Civil Liberties committee draft report on anti-radicalization, emphasize a stronger role for intermediaries in policing online content. See Commission, 'Proposal for a Directive on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA on Combating Terrorism' COM(2015) 0625 final (2 December 2015); European Parliament, 'Draft Report on Prevention of Radicalization and Recruitment of European Citizens by Terrorist Organizations' 2015/2063(INI) (1 June 2015); Home Department (UK), *Counter-Extremism Strategy* (Cmd 9148, 2015).

[164] See Commission, European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech, Press Release (31 May 2016) <http://europa.eu/rapid/press-release_IP-16-1937_en.htm>.

[165] ibid

[166] See 'Google in Europe, Partnering to Help Curb the Spread of Terrorist Content Online' (*Google Blog*, 5 December 2016) <https://blog.google/topics/google-europe/partnering-help-curb-spread-terrorist-content-online>.

have been using ContentID and other matching tools to filter "extremist content."[167] In this context, tech companies plan to create a shared database of unique digital fingerprints—known as ashes—that can identify images and videos promoting terrorism.[168] This could include recruitment videos or violent terrorist imagery or memes. When one company identifies and removes such a piece of content, the others will be able to use the hash to identify and remove the same piece of content from their own network. The fingerprints will help identify image and video content that are 'most likely to violate all of our respective companies' content policies'.[169] Despite the collaboration, the task of defining removal policies will remain within the remit of each platform.[170]

However, a report from the European Commission on the implementation of the Code of Conduct on Illegal Hate Speech EU highlighted that the compliance with the code is still far yet from satisfactory.[171] The Commission stressed the need for internet platforms to speed up the removal process of hate speech, under the penalty of legislative action or legal pursuit.[172] Automatic recognition technologies do become a privileged tool to prevent terrorist propaganda. The Communication *Tackling Illegal Content Online* reinforces this point on the agenda by endorsing "automatic stay-down procedures" to fingerprint and filter out content which has been [**26**] already identified and assessed as illegal.[173] In addition, especially in the domain of terrorist propaganda, extremism, and hate speech, as mentioned, online platforms must promote faster take-down mechanisms with 'trusted flaggers' and user-friendly anonymous notification systems.[174]

Because self-regulations expected by governments appears to lag behind, some EU member States such as Germany have threaten to bring in a law to impose heavy

---

[167] See Joseph Menn and Dustin Volz, 'Exclusive: Google, Facebook Quietly Move Toward Automatic Blocking of Extremist Videos' (*Reuters*, 25 June 2016) <http://www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M> (apparently, the "automatic" removal of extremist content is only about automatically identifying duplicate copies of video that were already removed through human review).

[168] Olivia Solon, 'Facebook, Twitter, Google and Microsoft Team up to Tackle Extremist Content (*The Guardian*, 6 December 2016) <https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content>.

[169] See 'Partnering to Help Curb Spread of Online Terrorist Content' (*Facebook Newsroom*, 5 December 2016) <https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content>.

[170] ibid

[171] See Commission, Justice and Consumers, Fighting Illegal Online Hate Speech: First Assessment of the New Code of Conduct, Press Release (12 December 2016), <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50840>.

[172] ibid

[173] See Communication (n 30) § 5.2.

[174] ibid § 3.2.1. and 3.2.3.

fines on a platform failing to take down hate-based criminal content.[175] The German government introduced a *Draft Law to Improve Law Enforcement in Social Networks*--abbreviated as the Network Enforcement Act (Netzwerkdurchsetzungsgesetz), or NetzDG.[176] The proposed legislation would apply to social networks and specifically exclude news platforms.[177] Social networks—which need at least 2 million registered users in Germany to qualify—are defined as (i) providers of telemedia services that, (ii) for purposes of generating profit, (iii) operate platforms in the Internet, which (d) permit users share content, to make content public, or to exchange content with other users.[178] "Obviously unlawful" content—which encompasses fourteen specific crimes set forth in the German Criminal Code[179]—must be evaluated and removed within 24 hours from a complain.[180] The law would impose stay-down obligations as the social network must remove all other copies of the illegal content from the network and implement effective measures to prevent the illegal content from being re-posted.[181] Violating takedown requirements would cost up to €500,000 in fines for individuals and up to €5,000,000 for companies.[182] These fines might be far-reaching and cover also search engines, listing for examples links to Holocaust-denial articles, which are prohibited speech covered by Section 130(3) of the German Criminal Code.[183] Meanwhile, German prosecutors in Munich are investigating Facebook executives, following a complaint alleging the company broke national laws against hate speech

---

[175] See Cara McGoogan, 'German Politician Threatens to Fine Facebook €500,000 Every Time It Shows Fake News' (*The Telegraph*, 19 December 2016) <http://www.telegraph.co.uk/technology/2016/12/19/ger man-politician-threatens-fine-facebook-500000-every-time>.

[176] See Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) (14 March 2017) <http://www.alstonprivacy.com/wp-content/uploads/2017/03/2017-03-14-NetzDG_Entwurf-des-BMJV.pdf> [hereinafter NetzDG]. See *also* Daniel Felz, 'Germany Proposes Bill Requiring Social Network Takedowns – with € 50 Million Fines' (*Alston&Bird*, 14 March 2017) <http://www.alstonprivacy.com/german-justice-department-publishes-bill-requiring-social-networks-implement-takedown-procedures-illegal-content-work-law-enforcement-subject-e-50-million-fines>; Wolfgang Schulz, 'Comments on the Draft for an Act Improving Law Enforcement on Social Networks (NetzDG)' <http://www.hans-bredow-institut.de/webfm_send/1178>.

[177] See NetzDG (n 176) § 1(1-2).

[178] ibid

[179] ibid § 1(3).

[180] ibid § 3(2)2.

[181] ibid § 3(2)6-7.

[182] ibid, at § 4(2).

[183] See Philip Oltermann, 'Germany to Force Facebook, Google and Twitter to Act on Hate Speech' (*The Guardian*, 17 December 2016) <https://www.theguardian.com/technology/2016/dec/17/german-officials-say-facebook-is-doing-too-little-to-stop-hate-speech>.

and sedition by failing to remove racist [**27**] postings.[184] Complaints have been filed also in Hamburg, where however prosecutors rejected them on the grounds that the regional court lacked jurisdiction because Facebook's European operations are based in Ireland.[185]

Online Search Manipulation

Online search manipulation—and so-called demotion—enforce sanitization of presumptively illicit activities online through voluntary measures and private ordering. This regulatory approach also spans multiple subject matters and online allegedly illicit activities. Copyright enforcement online have a primary goal of search manipulation. Starting from the most recent effort of this kind, under the aegis of the UK Intellectual Property Office, search engines and the creative industries concluded an agreement to stop consumers being led to copyright infringing websites.[186] Representatives from the creative industries, leading UK search engines, and the IPO developed a Voluntary Code of Practice dedicated to the removal of links to infringing content from the first page of search results.[187] The Code—which came immediately into force—sets targets for reducing the visibility of infringing content in search results by 1 June 2017. However, Google have been demoting allegedly pirate sites for some time now. In 2012, Google altered it PageRank search algorithm taking into account the number of DMCA-compliant notices for each website.[188] Shortly thereafter, in 2014, Google started to demote autocomplete predictions returning search results containing DMCA-demoted sites.[189] Apparently, the demotion and search manipulation tools that Google implemented proved ineffective as claimed by a RIAA and MPAA

Voluntary measures have been traditionally implemented with regard to manifestly illegal content, such as child pornography.[190] Platforms' involvement in curbing online pornography have been increasingly sought also for revenge porn—another behaviour characterized by high social disapproval. Suzor, Seignior and Singleton have argued that 'the challenge in developing effective policy is not only

---

[184] See 'Here's Why German Prosecutors Are Investigating Facebook and Mark Zuckerberg' (*Fortune*, 4 November 2016) <http://fortune.com/2016/11/04/germany-facebook-zuckerberg/?xid=soc_socialflow_twitter_FORTUNE>

[185] ibid

[186] See Intellectual Property Office, 'Press Release: Search Engines and Creative Industries Sign Anti-Piracy Agreement' (20 February 2017) <https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement>.

[187]

[188] See Bridy (n 111) 200.

[189] ibid

[190] See Anchayil Anjali, and Arun Mattamana, 'Intermediary Liability and Child Pornography A Comparative Analysis' (2010) 5 J Int'l Comm L Tech 48.

to provide a remedy against the primary wrongdoer, but to impose some obligations on the platforms that host or enable access to harmful material'.[191] Rather than waiting for legislatively mandated obligations, online hosting providers have been increasingly pursuing self-regulatory initiatives in this field. Recently, Google has adopted specific [**28**] self-regulatory measures for revenge porn, which Google delists from Internet searches.[192] The close resemblance between Google voluntary actions to curb revenge porn online and the right to be forgotten is obvious.[193] Other major platforms followed Google's lead. After being ordered by a Dutch court to identify revenge porn publishers in the past,[194] Facebook decided to introduce photo-matching technology to stop revenge porn and proactively filter its reappearance.[195]

Finally, search manipulation and demotion begun to be applied to curb extremism and radicalization. Plans have been also revealed of a pilot scheme to tweak search to make counter-radicalisation videos and links more prominent.[196]

Payment Blockades and Follow the Money

Payment blockades—notice-and-termination agreement between major right holders and online payment processors—and "voluntary best practices agreements" have been applied widely—especially in the United States—as part of 'a long-term, evolving strategy on the part of corporate copyright and trademark owners'.[197] Payment processors like MasterCard and Visa have been pressured to act as intellectual property enforcers, extending the reach of intellectual property law to websites operating from servers and physical facilities located abroad.[198] As

---

[191] See Nicolas Suzor, Bobbie Seignior and Jen Singleton, 'Non-consensual Porn and the Responsibility of Online Intermediaries' (2017) 40(3) Melbourne U L Rev (forthcoming).

[192] See Joanna Walters, 'Google to Exclude Revenge Porn from Internet Searches? (*The Guardian*, 21 June 2015) <https://www.theguardian.com/technology/2015/jun/20/google-excludes-revenge-porn-internet-searches>. See also

[193] See Woodrow Hartzog and Evan Selinger, 'Google's Action on Revenge Porn Opens the Door on Right to be Forgotten in US' (*The Guardian*, 21 June 2015) <https://www.theguardian.com/technology/2015/jun/25/googles-revenge-porn-opens-right-forgotten-us>.

[194] See Agence France-Press, 'Facebook Ordered by Dutch Court to Identify Revenge Porn Publisher' (*The Guardian*, 26 June 2015) <https://www.theguardian.com/technology/2015/jun/26/facebook-ordered-by-dutch-court-to-identify-revenge-porn-publisher>.

[195] Emma Grey Ellis, 'Facebook's New Plan May Curb Revenge Porn, but Won't Kill It' (*Wired*, 6 April 2017)

[196] See Ben Quinn, 'Google to Point Extremist Searches Towards Anti-radicalization Websites' (*The Guardian*, 2 February 2016) <http://buff.ly/20J3pFi>.

[197] See Annemarie Bridy, 'Internet Payment Blockades' (2015) 67 Florida L Rev 1523.

[198] See Bridy (n 197) 1523. See Also Backpage v. Dart (denying an injunction against Sheriff Dart for his informal efforts to coerce credit card companies into closing their accounts with Backpage).

Annemarie Bridy argues, 'non-regulatory intervention from the executive branch secured [payment processors'] cooperation as a matter of private ordering'.[199]Across 2011 and 2012, American Express, Discover, MasterCard, Visa, and PayPal, PULSE, and Diners Club entered into a best practice agreement with thirty-one major right holders.[200] The voluntary agreement was implemented by the lunch of the Payment Processor Initiative run by the International AntiCounterfeiting Coalition (IACC).[201] The role of the IACC resembles closely that of the Center for Copyright information formerly administering the CAS graduated response system.[202] [**29**]

PayPal also have taken upon itself the duty of policing the internet by banning payments to VPN providers and geoblocking-circumvention services on 'copyright grounds'.[203] Apparently, by making more difficult to process payments with VPN's services—although using a VPN is not illegal—PayPal would like to curb the practice of using VPN to avoid geo-blocking restriction imposed on users by services like Netflix. According to PayPal, payment processing agreements were severed unilaterally with VPN providers because its services cannot be used to 'send or receive payments for items that infringe or violate any copyright, trademark, right of publicity or privacy, or any other proprietary right under the laws of any jurisdiction'. [204] PayPal practice—apparently occurring in Australia where users broadly use VPNs as they face major limitations in accessing Netflix's catalogue—clearly highlights tensions with fundamental rights that would impose non-discrimination obligations on technologically neutral services.

In its most recent Joint Strategic Plan for Intellectual Property Enforcement—titled *Supporting Innovation, Creativity & Enterprise: Charting a Path Ahead*—the US Government backed-up voluntary measures and fully endorsed a 'follow the money' strategy.[205] It states explicitly that .an effective enforcement strategy against commercial-scale piracy and counterfeiting therefore, must target and dry up the illicit revenue flow of the actors engaged in commercial piracy online'.[206] According

[199] Bridy (n 197) 1523 (also suggesting, however, that 'payment blockades can be circumvented with the aid of disintermediating technologies [. . .] P2P virtual currencies like Bitcoin are empowering online merchants and their customers, at least for the time being, to run payment blockades').

[200] See Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet (16 May 2011).

[201] See Bridy (n 96) 1549.

[202] ibid

[203] Rae Johnson, PayPal Is Blocking Payments To VPN Providers' (Gizmodo, 10 February 2016) <https://www.gizmodo.com.au/2016/02/paypal-is-blocking-payments-to-vpn-providers> (including a copy of the termination letter sent by PayPal to UnoTelly—an Australian VPN).

[204] ibid

[205] See Supporting Innovation, Creativity & Enterprise: Charting a Path Ahead (U.S. Joint Strategic Plan for Intellectual Property Enforcement FY 2017-2019).

[206] ibid 61.

to the Joint Strategic Plan, this revenue should be cut-off through voluntary collaboration between payment processors, online advertisers, and the banking sector.[207] In particular, the US Government wold like to push self-regulation and private enforcement to asphyxiate 'Ad revenue [. . .] the oxygen that allows content theft to breathe'.[208] To that end, 'IPEC and the IPR Center (with its constituent law enforcement partners), along with other relevant Federal agencies, will convene the advertising industry to hear further about their voluntary efforts'.[209]

In the Communication *Towards a Modern, More European Copyright Framework*, the Commission apparently would like to endorse similar strategies by deploying a 'follow-the-money' approach.[210] As the Commission noted, this strategy 'can deprive those engaging in commercial infringements of the revenue streams (for example from consumer payments and advertising) emanating from their illegal activities, and therefore act as a deterrent'.[211] According to the Commission, 'follow-the-money' mechanism should be based on a self-regulatory approach through the [**30**] implementation of Code of Conducts that might be later backed up by legislation if necessary.[212] In compliance with this agenda—in October 2016—the Commission agreed on the Guiding Principles for a *Stakeholders' Voluntary Agreement on Online Advertising and IPR*.[213] As stated by the principles, "the purpose of the agreement is to dissuade the placement of advertising on commercial scale IP infringing websites and apps (e.g. on mobile, tablets, or set-top boxes), thereby minimising the funding of IP infringement through advertising revenue."[214] Similar code of conduct and self-regulation have been already agreed upon by national governments in Europe, such as in Denmark or Belgium.[215]

Censorship pressures on financial intermediaries—credit card companies and third-party payment processors—have reached far beyond intellectual property infringement. In particular, there are a number of instances where payment

---

[207] ibid

[208] ibid 63.

[209] ibid 65.

[210] See Commission, 'Towards a Modern More European Copyright Framework' (Communication) COM (2015) 260 final 10-11.

[211] ibid 11.

[212] ibid

[213] Commission, 'The Follow the Money Approach to IPR Enforcement – Stakeholders' Voluntary Agreement on Online Advertising and IPR: Guiding Principles' http://ec.europa.eu/docsroom/documents/19462/attachments/1/translations/en/renditions/native.

[214] ibid

[215] See Danish Ministry of Culture, Code of Conduct to Promote Lawful Behaviour on the Internet (8 August 2015). See also Jesper Lund, 'Danish Ministry of Culture: Danes Should be Regulated by Google' (EDRi, 3 June 2015) <https://edri.org/danish-culture-ministry-danes-regulated-by-google>.

intermediaries' terms of service have been used as pressure points against protected speech. *Inter alia*, payment blockades crippled Wikileaks of 95% of its revenues, when PayPal, Moneybookers, Visa and MasterCard stopped accepting public donations. No legal proceeding was ever actually initiated against Wikileaks. In *Backpage v. Dart*, Backpage sought an injunction against Sheriff Dart for his informal efforts to coerce credit card companies into closing their accounts with the site. Sheriff Tom Dart—the sheriff for Cook County, Illinois—sent letters to Visa and MasterCard demanding that they cease doing business with Backpage.com due to content in the "adult services" section of the classified ads site.[216] The credit card companies both complied, cutting off services to the entire site's worldwide operations.[217] Backpage claimed that the sheriff's informal censorship pressure amounted to a prior restraint on speech.[218] Backpage was granted a temporary restraining order against the sheriff[219] but was denied a preliminary injunction at the district court.[220] The case was finally appealed to the Seventh Circuit, which reversed the previous decision and upheld a prior restraint on speech defence.[221] As it turned out, however, a single action from a governmental official—lacking any due process scrutiny—was potentially capable to put under jeopardy an online business operating worldwide. The [**31**] *Backpage* case highlights how intermediaries often face business incentives that make them more likely to yield to pressure. In the United States, a prior restraint on speech defence would not be directly actionable against intermediaries—if governmental pressures cannot be proved—as it does apply only against public parties. Under European law, there might be room to claim interference with online providers' freedom to conduct a business,[222] still this is costly and uncertain to prove.

[216] See Letter from Sheriff Thomas J. Dart to Mr. Charles W. Scharf, Chief Executive, Visa Inc. (29 June 2015) <http://cdn.arstechnica.net/wp-content/uploads/2015/07/backpageexhibit.pdf>; Letter from Sheriff Thomas J. Dart to Mr. Ajaypal Banga, President and Chief Executive Officer, MasterCard Inc. (29 June 2015)

[217] See Rainey Reitman, 'Caving to Government Pressure, Visa and MasterCard Shut Down Payments to Backpage.com? (*EFF*, 6 July 2015) <https://www.eff.org/deeplinks/2015/07/caving-government-pressure-visa-and-mastercard-shut-down-payments-backpagecom>.

[218] See Backpage.com v. Sheriff Thomas J. Dart, 1:15-cv-06340 (N.D. Ill. 2015) (Complaint for Injunctive and Declaratory Relief and Damages)

[219] See Backpage.com v. Sheriff Thomas J. Dart, 1:15-cv-06340 (N.D. Ill. 24 July 2015) (Order).

[220] See Backpage.com v. Sheriff Thomas J. Dart, 127 F.Supp.3d 919 (N.D. Ill. 2015).

[221] See Backpage.com v. Sheriff Thomas J. Dart, 807 F.3d 229 (7th Cir. 2015).

[222] *See* EU Charter (n 151) art 16.

Private DNS Content Regulation

Domain hopping—a tactic notoriously employed by The Pirate Bay[223]—would evade law enforcement by moving from one ccTLDs (country code Top-Level Domains) or gTLDs (Generic Top-Level Domains) registrar to another, thus driving up time and resources spent on protecting intellectual property right. In its Joint Strategic IP Enforcement Plan, the US government set as a priority to counter domain hopping and abusive domain name registration tactics.[224] In this respect, new voluntary online enforcement schemes would also rely on stewards of the Internet's core technical functions, such as ICANN, and implicates Internet infrastructure and governance. [225] Intellectual Property enforcement would occur at the Internet backbone through the administration of the Domain Name System (DNS).

Apparently, ICANN might be increasingly directly involved with online content regulation through its contractual facilitation of a 'trusted notifier' copyright enforcement program. ICANN contractual architecture for the new gTLDs embeds support for private, DNS-based content regulation on behalf of copyright holders—and, potentially, other 'trusted' parties—imposing on registry operators and registrars an express prohibition on copyright infringement and obligations including suspension of the domain name.[226] Though this contractual framework, ICANN facilitated voluntary enforcement agreements between DNS intermediaries and rightholders, such as the DNA's Healthy Domains Initiative. [227]According to specific program between the Motion Picture Association of America (MPAA) and two registry operators for new gTLDs, Seattle-based Donuts and Abu Dhabi-based Radix, registry operators are now acting as private copyright enforcers for 'trusted notifiers', which are broadly defined as 'an industry representative trade association that represents no [**32**] single company, [. . .] dedicated to examining illegal behavior, [. . .] with [. . .] ability to identify and determine the relevant category of illegal activity'.[228] Apparently, the ICANN's 'trusted notifier' model matches closely

---

[223] See Ernesto, Pirate Bay's Domain Shuffle Has Come Full Circle (*TorrentFreak*, 20 May 2016) <https://torrentfreak.com/pirate-bays-domain-shuffle-come-full-circle-160520>.

[224] See Supporting Innovation, Creativity & Enterprise (n 205) 68-69.

[225] See Annamarie Bridy, 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation' (2017) Washington and Lee L Rev (forthcoming) (SSRN draft).

[226] See ICANN-Registry Agreement (2013) § 2.17 Specification 11 (requiring registry operators to include in their contracts with registrars a provision requiring registrars to include in their contracts with registrants "a provision prohibiting Registered Name Holders from […] piracy, trademark or copyright infringement […] and providing [...] consequences for such activities including suspension of the domain name."); ICANN Registrar Accreditation Agreement (2013) § 3.18. See also Bridy (n 225) 16-20.

[227] See Meeting Transcript, MARRAKECH–Industry Best Practices–the DNA's Healthy Domains Initiative 13 <https://meetings.icann.org/en/marrakech55/schedule/wed-dna-healthy-domains-initiative/transcript-dna-healthy-domains-initiative-09mar16-en.pdf>. See also Bridy (n 225) 20.

[228] See Donuts.Domains, Characteristics of a Trusted Notifier Program <http://www.donuts.domains/images/pdfs/Trusted-Notifier-Summary.pdf>.

the 'trusted flaggers'—similarly defined as specialized private entities with specific expertise in identifying illegal content'—which, according to the most recent EU Commission's Communication on point, should enjoy a privileged channel with online intermediaries for removals of allegedly infringing content.[229] The registry operators agrees, if "the domain clearly is devoted to abusive behaviour [. . .] in its discretion [to] suspend, terminate, or place the domain on registry lock, hold, or similar status' within ten business days form the complaint.[230] Apparently, there are no due process safeguards for the registrar to receive notice of the complaint or respond.[231] In general, as Bridy explained, 'in creating that architecture, ICANN did nothing to secure any procedural protections or uniform substantive standards for domain name registrants who find themselves subject to this new form of DNS regulation'.[232]

IV. Conclusions

Intermediary responsibility has become the latest trend in online governance. Terminologically first, it is slowly displacing the notion of intermediary liability. Responsibility of intermediaries is all over the literature and a powerful slogan for policy makers. The European Commission have plainly admitted in recent documents that have been shaping the Digital Single Market to come that 'responsibility of online platforms is a key […] issue' and that the path is set "towards an enhanced responsibility of online platforms'. The new terminology, however, does represent a substantial shift in intermediary liability theory that apparently would move away from a well-established utilitarian approach toward a moral approach by rejecting negligence-based intermediary liability arrangements. In turn, this theoretical approach portends the enhanced involvement of private parties in online governance and a broader move towards private enforcement online. Public enforcement lacking technical knowledge and resources to address an unprecedented challenge in terms of global human semiotic behaviour would coactively outsource enforcement online to private parties.

The deployment of miscellaneous policy tools—such as graduated response, monitoring and filtering obligations, online search manipulation, payment blockades and follow-the-money strategies, and private DNS content regulation—reflects this change in perspective. In particular, increasingly, governments—and interested third-parties such as intellectual property rightholders—try to coerce online intermediaries into implementing this policy strategies through self-regulation and voluntary measures. Private ordering does become the privileged tool to enforce a responsible—and cooperative—behaviour of intermediaries. Nevertheless, intermediary responsibility also emerges from normative arrangements that make

[229] Communication (30) § 3.2.1.

[230] ibid

[231] See also Bridy (n 225) 20.

[232] ibid 29.

more prominent the role of online intermediaries, while incentivizing over-zealous [**33**] enforcement. This is apparently the case of blocking orders dealt almost entirely between intermediaries and righstholders and administrative enforcement of intermediary liability online.

Private ordering—and the retraction of the public from online enforcement—does push an amorphous notion of responsibility that incentivizes intermediaries' self-intervention to police allegedly infringing activities in the Internet. It highlights unescapable tensions with fundamental rights that would impose non-discrimination obligations on technologically neutral services capable of substantial non-infringing uses. Obviously, transferring regulation and adjudication of Internet rights to private actors does jeopardize fundamental rights—such as freedom of information, freedom of expression, freedom of business or a fundamental right to Internet access—by limiting access to information, causing chilling effects, or curbing due process. Further, enforcement would be looking once again for an 'answer to the machine in the machine'. By enlisting online intermediaries as watchdogs, governments would *de facto* delegate online enforcement to algorithmic tools. Due process and fundamental guarantees get mauled by technological enforcement, curbing fair uses of content online and silencing speech according to the mainstream ethical discourse. The response to the centrifugal move caused by private ordering and intermediary responsibility should be a centripetal reaction towards Internet Bills of Rights, Internet Constitutional Charts and mandatory Internet Governance and Intermediary Liability Principles. Digital constitutionalism—although partially occurring at multiple levels—seems overshadow for now by the counterpoising trend that this article detailed.