Internet Intermediary Liability: WILMap, Theory and Trends

Giancarlo F. Frosio[*]

Abstract *To better understand the heterogeneity of the international online intermediary liability regime—with the collaboration of an amazing team of contributors across five continents—I have developed and launched the World Intermediary Liability Map (WILMap), a detailed English-language resource, hosted at Stanford CIS and comprising of case law, statutes, and proposed laws related to intermediary liability worldwide. Since its launch in July 2014, the WILMap has been steadily and rapidly growing. Today, the WILMap covers almost one hundred jurisdictions across Africa, Asia, the Caribbean, Europe, Latin America, North America and Oceania. This article begins with an introduction of the WILMap and the surrounding landscape of recent projects related to intermediary liability. The aim is to discuss the advancement in intermediary liability theory and describing the emerging regulatory trends.*

I. Introduction

It is not surprising that online intermediaries' obligations, liabilities, and responsibilities are increasingly taking the center stage of Internet policy. However, inconsistencies across different regimes generate legal uncertainties that undermine both users' rights and business opportunities. To better

[*] 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.

understand the heterogeneity of the international online intermediary liability regime—with the collaboration of an amazing team of contributors across five continents—I have developed and launched the World Intermediary Liability Map (WILMap), a detailed English-language resource, hosted at Stanford CIS, comprising of case law, statutes, and proposed laws related to intermediary liability worldwide.[1]

Mapping online intermediary liability worldwide serves the goal of understanding responsibilities that online service providers (hereinafter, "OSPs") bear in contemporary information societies. Most creative expression today takes place over communication networks owned by private companies. OSPs' role is unprecedented due to 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*" (hereinafter, "RTBF").

Mapping online intermediary liability worldwide entails the review of a wide-ranging topic, stretching into many different areas of law and domain-specific solutions. The WILMap has become a privileged venue to observe emerging trends in Internet jurisdiction and innovation regulation, enforcement strategies dealing with intermediate liability for copyright, trademark, and privacy (RTBF) infringement, and the role of Internet platforms in moderating the speech they carry for users, including obligations and liabilities for defamation, hate and dangerous speech. Such mapping is expected to help in focusing on gaps in policies and existing legal frameworks regulating OSPs, and provide possible strategies to overcome it.

II. The WILMap Project

By their very nature, Internet services are inherently global, but Internet companies face a real challenge in understanding how those global regimes might regulate the services they offer to the public. In search for consistency—and to contribute to this important policy debate—I developed the World Intermediary Liability Map (WILMap), a repository of information on international liability regimes.[2] The WILMap is a graphic interface for

[1] World Intermediary Liability Map (WILMap), https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap [hereinafter, "WILMap"].

[2] The Stanford Intermediary Liability Lab (SILLab), another project I launched at Stanford Law School in 2013, functioned as an incubator for developing the WILMap and studying international approaches to intermediary obligations concerning users' copyright

legislation and case law enabling the public to learn about intermediary liability regimes worldwide and the evolving Internet regulations affecting freedom of expression and user rights. This detailed English-language resource allows visitors to select information on countries of interest, including case law, statutes, and proposed laws. Each country page includes links to original sources and English translations, if available. As the WILMap website clearly states, this resource should be used "to learn about intermediary liability regimes worldwide, and to identify places where legal regimes balance—or fail to balance—regulatory goals with free expression and other civil liberties."[3]

The WILMap features legislation, pending bills and proposals imposing obligations on intermediaries, both access and hosting providers or other online intermediaries, such as payment processors. The WILMap covers wide-ranging topics, including online intermediaries' safe harbors, e-commerce, copyright and trademark protection, defamation, hate/dangerous speech, including anti-terrorism provisions, privacy protection, and child protection online. If available, the WILMap provides relevant case law for each jurisdiction. Basically, the WILMap aims to feature case laws discussing obligations and liability of online intermediaries due to (infringing) activities undertaken by their users. The WILMap also features sections for administrative enforcement of intermediary liability online, if there are administrative agencies responsible for implementing website blocking orders or content removal in a particular jurisdiction.

Since its launch in July 2014, the WILMap has been steadily and rapidly growing. Today, the WILMap covers almost one hundred jurisdictions across Africa, Asia, the Caribbean, Europe, Latin America, North America and Oceania. The WILMap is an ongoing project. In collaboration with a network of experts worldwide, the Center for Internet and Society (CIS) continues to update and expand the map so as to cover all jurisdictions. In an effort to make the WILMap an increasingly valuable resource for activists, industry players, researchers, and the general public, the WILMap website will soon be updated with enhanced usability and data aggregation features.

The WILMap project is the result of the inputs of an amazing team of contributors from around the world, both individual researchers and institutions, who provided the necessary information to create and update each

---

infringement, defamation, hate speech or other vicarious liabilities, immunities, or safe harbours. *See* Stanford Intermediary Liability Lab, https://www.facebook.com/groups/ILLab; *see also* CIS, Intermediary Liability, https://cyberlaw.stanford.edu/focus-areas/intermediary-liability.

[3] Homepage, WILMap, *supra* note 1.

country page. The creation of a global network of WILMap contributors also allowed promotion of synergy with global platforms and free expression groups to advocate for policies aimed at protection of innovation and other user rights.[4]

III. Other Intermediary Liability Projects

The WILMap's attempt to study intermediary liability, in order to come to terms with a fragmented legal framework, is not isolated. Mapping and comparative analysis exercises have also been undertaken by the Network of Centers (which produced a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union (EU), India, South Korea, the United States (US), Thailand, Turkey, and Vietnam),[5] WIPO,[6] and other academic initiatives.[7]

Institutional efforts at the international level are on the rise. Recently, the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) worked towards the establishment of global provisions on intermediary liability within a charter of Internet governance principles.[8] The final text of the NETmundial Statement included the principle that,

---

[4] *See* OSJI-CIS Workshop on Intermediary Liability, Fostering Greater Collaboration between Service Providers and Internet Freedom Groups in the Public Interest, Stanford University, Stanford, CA, December 15, 2014.

[5] *See* Berkman Center for Internet and Society, Liability of Online Intermediaries: New Study by the Global Network of Internet and Society Centers, February 18, 2015, https://cyber.law.harvard.edu/node/98684; Urs Gasser and Wolfgang Schulz, Governance of Online Intermediaries: Observations from a Series of National Case Studies (Berkman Center Research Publication No. 2015-5, 2015), http://ssrn.com/abstract=2566364.

[6] *See* Daniel Seng, Comparative Analysis of National Approaches to the Liability of the Internet Intermediaries, VII. Japan (WIPO Study), *available at* http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf; Ignacio Garrote Fernández-Díez, Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights (WIPO study), *available at*http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf.

[7] *See*, *e.g.*, for other mapping and comparative exercises, Intellectual Property Liability of Consumers, Facilitators, and Intermediaries (Christopher Heath and Anselm Kamperman Sanders (eds.), Wolters Kluwer 2012).

[8] *See* NETmundial Multistakeholder Statement, São Paulo, Brazil, April 24, 2014, *available at*http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; *see also* Nicolo Zingales, *The Brazilian Approach to Internet Intermediary Liability: Blueprint for a Global Regime*, 4(4) Internet Policy Rev. (December 28, 2015), http://policyreview.info/articles/analysis/brazilian-approach-internet-intermediary-liability-blueprint-global-regime (noting that this formulation is problematic for civil society because of the focus on economic aspects – and rightholders' interests – rather than on protection of human rights); Marilia Maciel, Nicolo Zingales, and Daniel Fink, The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial),

"*Intermediary liability limitations should be implemented in a way that respects and promotes economic growth, innovation, creativity and free flow of information. In this regard, cooperation among all stakeholders should be encouraged to address and deter illegal activity, consistent with fair process.*"[9]

A few months earlier, the Organization for Economic Co-operation and Development (OECD) issued recommendations on Principles for Internet Policy Making stating that, in developing or revising their policies for the Internet Economy, the State members should consider the limitation of intermediary liability as a high level principle.[10] Moreover, the 2011 Joint Declaration of the three Special Rapporteurs for Freedom of Expression contains statements that would suggest an ongoing search for a global regime for intermediary liability.[11] After reinforcing the mere conduit principle, the declaration suggested liability limitations for other intermediaries, including hosting providers, search engines, and those enabling financial transactions.[12] The Representative on Freedom of the Media of the Organization for Security and Cooperation in Europe (OCSE) issued a *Communiqué on Open Journalism*, which is aimed at advising the organization's 57 member States on best practices with regards to digital rights and intermediaries.[13] In particular, the Communiqué laid out a set of recommendations in recognition of the fact that "*intermediaries have become one of the main platforms*

---

case study by the Center for Technology and Society of the Getulio Vargas Foundation (2014), https://publixphere.net/i/noc/page/IG_Case_Study_NETMundial.

9 *Id*., at 5.

10 *See* Organization for Economic Co-operation and Development (OECD), Recommendation of the Council on Principles for Internet Policy Making, C (2011) 154 (November 13, 2011), *available at* http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=270; *see also* OECD, The Economic and Social Role of Internet Intermediaries (April 2010), *available at* http://www.oecd.org/internet/ieconomy/44949023.pdf [hereinafter, "OECD, Internet Intermediaries"].

11 *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 (June 2011), *available at* http://www.osce.org/fom/78309?download =true [hereinafter, "Joint Declaration of the Three Special Rapporteurs for Freedom of Expression"].

12 *Id*., at Preamble and 2.b.

13 Organization for Security and Cooperation in Europe (OCSE) The Representative on Freedom of the Media, Dunja Mijatović, 3rd Communiqué on Open Journalism, Vienna, January 29, 2016, http://www.osce.org/fom/219391?download=true [hereinafter, "OCSE, Communiqué on Open Journalism"].

facilitating access to media content as well as enhancing the interactive and participatory nature of Open Journalism."[14]

Efforts to produce guidelines and general principles for intermediaries emerged in the civil society too. In particular, the Manila Principles on Intermediary Liability set out safeguards for content restriction on the Internet with the aim of protecting users' rights, including "*freedom of expression, freedom of association and the right to privacy*."[15] A set of general principles is accompanied by sub-principles and a background paper qualifying some of the terminology and statements included in the principles.[16] The six main principles are summarized below:

> "(1) Intermediaries should be shielded from liability for third-party content. (2) Content must not be required to be restricted without an order by a judicial authority. (3) Requests for restrictions of content must be clear, be unambiguous, and follow due process. (4) Laws and content restriction orders and practices must comply with the tests of necessity and proportionality. (5) Laws and content restriction policies and practices must respect due process. (6) Transparency and accountability must be built into laws and content restriction policies and practices."[17]

The Manila Principles have been well received so far by the international community. For example, institutional initiatives such as the OCSE Communiqué on Intermediaries mentioned before made full reference to the Manila Principles in its draft recommendations.[18]

Other projects have developed best practices that might be implemented by intermediaries in their Terms of Service with special emphasis on protecting fundamental rights.[19] For example, under the aegis of the Internet Governance Forum, the Dynamic Coalition for Platform Responsibility

---

[14] *Id*.

[15] *See* Manila Principles on Intermediary Liability, Intro, https://www.manilaprinciples.org/.

[16] *See* Manila Principles on Intermediary Liability Background Paper (May 30, 2015), https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf; Jyoti Panday, Carlos Lara, Kyun Park, and Kelly Kim, Jurisdictional Analysis: Comparative Study Of Intermediary Liability Regimes Chile, Canada, India, South Korea, UK and USA in support of the Manila Principles on Intermediary Liability (July 1, 2015), https://www.eff.org/files/2015/07/08/manila_principles_jurisdictional_analysis.pdf.

[17] *Id*.

[18] *See* OCSE, Communiqué on Open Journalism, *supra* note 13, at 2.

[19] *See*, *e.g.*, Jamila Venturini, Luiza Louzada, and Marilia Maciel, Terms of Service and Human Rights: An Analysis of Online Platform Contracts (Editora Revan 2016).

aims to delineate a set of model contractual provisions.[20] These 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.[21] 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 securing the respect of human rights in a responsible manner.*"[22] Further, the Global Network Initiative (GNI) put together a multistakeholder 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 communication 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 and Learning Framework.[23]

Ranking Digital Rights is an additional initiative that promotes best practices and transparency among online intermediaries.[24] This project ranks Internet and telecommunication companies according to their virtuous behaviour in respecting users' rights, including privacy and freedom of speech. In November 2015, the project's report ranked 16 companies, in different countries, on 30 different measures.[25] Companies scored between 65 and 13 percent.[26] Most companies received a failing grade for their public commitments and disclosed policies affecting users' freedom of expression and privacy.[27]

---

[20] *See* Dynamic Coalition on Platform Responsibility: A Structural Element of the United Nations Internet Governance Forum, http://www.intgovforum.org/cms/2008-igf-hyderabad/event-reports/74-dynamic-coalitions/1625-dynamic-coalition-on-platform-responsibility-dc-pr [hereinafter, "Dynamic Coalition on Platform Responsibility"].

[21] *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), *available at* http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf [hereinafter, "UN GPBHRs"].

[22] *See* Dynamic Coalition on Platform Responsibility, *supra* note 20.

[23] *See* Global Network Initiatives, Principles, https://globalnetworkinitiative.org/principles/index.php; Global Network Initiatives, Implementation Guidelines, https://globalnetworkinitiative.org/implementationguidelines/index.php; Global Network Initiatives, Accountability, Policy, and Learning Framework, https://globalnetworkinitiative.org/content/accountability-policy-and-learning-framework.

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

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

[26] *Id.*

[27] *Id.*

Several initiatives have been looking into notice and takedown procedures in order to highlight possible chilling effects and propose solutions. Lumen—formerly "*Chilling Effects*"—archives takedown notices to promote transparency and to facilitate research about the takedown ecology.[28] The Takedown Project is a collaborative effort housed at UC-Berkeley School of Law and the American Assembly to study notice and takedown procedures.[29] The Takedown Project launched the Notice Coding Engine to look at the impact of automated sending and receiving process of notice and takedown.[30] Apart from this, the Internet and Jurisdiction project has been developing a due process framework to deal more efficiently with transnational notice and takedown requests, seizures, MLAT and law enforcement cooperation requests.[31] This framework will be based on the creation of a legal reference database to support the assessment of takedown requests.[32] Finally, apart from establishing good practice standards for notices, the Manila Principles initiatives made available a template notice of content restriction as a mock-up web form that can be adopted by intermediaries.[33]

IV. From Intermediary Liability to Responsability

Intermediary liability has become one of the most critical Internet governance issues of our time. In particular, modern theory—and policy—still struggles with defining an adequate framework for the liability and responsibility of

---

[28] *See* Lumen, www.lumendatabase.org; *see also* Online Censorship, https://onlinecensorship.org (allowing users to document their experience with Terms of Service based removals of content).

[29] *See* The Takedown Project, http://takedownproject.org; *see also* Brianna L. Schofield and Jennifer M. Urban, Takedown and Today's Academic Digital Library, UC Berkeley Public Law Research Paper No. 2694731, 2015, *available at* http://ssrn.com/abstract=2694731 (examining academic libraries' interaction with DMCA and non-DMCA takedown requests); Annemarie Bridy, *Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries*, *in* Research Handbook on Electronic Commerce Law (John A. Rothchild (ed.), Edward Elgar 2016), *available at* http://ssrn.com/abstract=2628827 (surveying cooperative enforcement measures beyond what the DMCA requires by both intermediaries that are eligible for Section 512 safe harbours and those that are not liable under secondary liability doctrines); Daniel Seng, *The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices*, 18 Virginia J. L. & Tech. 369 (2014), *available at* http://ssrn.com/abstract=2411915 (charting a 711,887 percent increase in DMCA notices received by Google over the time of the study after analyzing half a million takedown notices and more than 50 million takedown requests).

[30] The Takedown Project, Projects, Notice Coding Engine, http://takedownproject.org/projects.

[31] *See* Bertrand de La Chapelle and Paul Fehlinger, Towards a Multi-Stakeholder Framework for Transnational Due Process (Internet & Jurisdiction White Paper, 2014), http://www.internetjurisdiction.net/uploads/pdfs/Papers/Internet-Jurisdiction-White-Paper-2014.pdf.

[32] *Id*.

[33] Template Notice Pre-Zero Draft Revised, https://goo.gl/NlVXEF.

OSPs for user-generated content. Does OSP's role differ from that of publishers, mass-media, and gate-keepers? Should innocent third parties be enlisted in online enforcement? If so, what are the jurisdictional boundaries of their obligations? These are some tough questions that have received miscellaneous answers so far even within a single jurisdiction. The theoretical—and market—background against which the intermediary liability debate developed has changed considerably since the first appearance of online intermediaries almost two decades ago. These changes reflected—or will, most likely, soon reflect—in changing policy approaches.

In the mid-nineties, after initial brief hesitation,[34] legislators decided that online intermediaries, both access and hosting providers, had to enjoy exemptions from liability for wrongful activities committed by users through their services. The safe harbors were first introduced by the United States. In 1996, the Communications Decency Act exempted intermediaries from liability for the speech they carried.[35] In 1998, the Digital Millennium Copyright Act introduced specific intermediary liability safe harbours for copyright infringement under more stringent requirements.[36] Shortly thereafter, the eCommerce Directive imposed an obligation on the member States to enact similar legal arrangements to protect a range of online intermediaries from liability.[37] Other jurisdictions have followed suit in more recent times.[38] In most cases, safe harbour legislations provide mere conduit, cach-

---

[34] *See* Bruce A. Lehman, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights 114-124 (DIANE Publishing, 1995), *available at* https://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf (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.

[35] *See* Communications Decency Act, 1996, 47 U.S.C. § 230, https://cyberlaw.stanford.edu/page/wilmap-united-states; *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*, 43 Loyola L. Rev. 373 (2010).

[36] *See* The Digital Millennium Copyright Act, 1998, 17 U.S.C. § 512, https://cyberlaw.stanford.edu/page/wilmap-united-states [hereinafter, "DMCA"].

[37] *See* Directive 2000/31/EC of the European Parliament and of the Council of June 8, 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"], *available at* http://cyberlaw.stanford.edu/page/wilmap-european-union.

[38] *See*, *e.g.*, Copyright Legislation Amendment Act, 2004 (Cth), No. 154, Sch. 1 (Australia), https://cyberlaw.stanford.edu/page/wilmap-australia; Copyright Modernization Act, SC 2012, c20, § 31.1 (Canada), http://cyberlaw.stanford.edu/page/wilmap-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), http://cyberlaw.stanford.edu/page/wilmap-china; Federal Law No. 149-FZ, on Information, Information Technologies and Protection of Information, July 27, 2006 (Russia) and Federal Law No.

ing, 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 to actively seek facts or circumstances indicating illegal activity.[39]

Pressurizing innocent third parties that may enable or encourage violations by others is a well-established strategy to curb infringement. In fact, 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.[40] The second approach is associated with the welfare theory and, more broadly, with a 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 in shaping early online intermediaries' policies.[41] Welfare theory approaches have been dominant in intermediary liability policy until recently. They have been based on the notion that liability should be imposed only as a result of a cost-benefit analysis, which is especially relevant in case of dual-use technologies that can be deployed both to infringe others' rights and facilitate social beneficial uses.[42]

Apparently, however, there is an ongoing 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 due to their capacity to influence the

187-FZ of July 2, 2013 amending Russian Civil Code, § 1253.1, http://cyberlaw.stanford.edu/page/wilmap-russia.

[39] *See*, *e.g.*, eCommerce Directive, *supra* note 37, at Art. 12-15; DMCA, *supra* note 36, at § 512(c)(1)(A-C).

[40] *See* Richard A. Spinello, *Intellectual Property: Legal and Moral Challenges of Online File Sharing*, *in*Ethics and Emerging Technologies 300 (Ronald L. Sandler (ed.), Palgrave Macmillan 2013); Mohsen Manesh, *Immorality of Theft, the Amorality of Infringement*, Stan. Tech. L. Rev. 5 (2006), *available at* https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review-stlr/online/manesh-immorality.pdf; Richard A. Spinello, *Secondary Liability in the Post Napster Era: Ethical Observations on MGM v. Grokster*, 3(3) J. of Information, Communication and Ethics in Society 121 (2005); Geraldine Szott Moohr, *The Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory*, 83 B.U. L. Rev. 731 (2003).

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

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

informational environment and the users' interactions within it. This move from intermediary liability to platform responsibility has been occurring at both theoretical and practical level, with special focus on intermediaries' corporate social responsibilities and their role in implementing and fostering human rights.[43] As Martin Husovec argued, the EU law, for example, increasingly forces Internet intermediaries to work for the right holders by making them accountable even if they are not tortiously liable for actions of their users.[44]

However, there are also 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.[45] 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 constitutionalism*."[46] These initiatives have great differences—and 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.[47]

---

[43] *See* Emily B. Laidlaw, Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility (CUP 2015); Mariarosaria Taddeo and Luciano Floridi, *The Debate on the Moral Responsibilities of Online Service Providers*, 22(6) Sci. & Eng. Ethics 1575 (published online November 27, 2015), *available at* http://link.springer.com/article/10.1007%2Fs11948-015-9734-1; Marcelo Thompson, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, 18(4) Vand. J. Ent. & Tech. L. (forthcoming 2016); Sophie Stalla-Bourdillon, *Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the e-Commerce Directive as Well...*, *in* The Responsibilities of Online Service Providers (L. Floridi and M. Taddeo (eds.), Springer 2016), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2808031; see also United Nations Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/26/13 (June 20, 2014), *available at* http://hrlibrary.umn.edu/hrcouncil_res26-13.pdf (addressing *inter alia* a legally binding instrument on corporations' responsibility to ensure human rights).

[44] *See* Martin Husovec, Accountable, Not Liable: Injunctions Against Intermediaries, TILEC Discussion Paper No. 2016-012 (May 2, 2016), *available at* 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.

[45] *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), *available at* http://ssrn.com/abstract=2687120.

[46] *See* Gill, Redeker, and Gasser, *supra* note 45, at 1.

[47] *See* Gill, Redeker, and Gasser, *supra* note 45, at 1.

V. Global Intermediary Liability Trends

Mapping online intermediary liability worldwide entails the review of a wide-ranging topic, stretching into many different areas of law and domain-specific solutions. The WILMap has become a privileged venue to observe emerging trends in Internet jurisdiction and innovation regulation, enforcement strategies dealing with intermediate liability for copyright, trademark, and privacy (RTBF) infringement, and Internet platforms' obligations and liabilities for defamation, hate and dangerous speech. The data set collected in the WILMap has made it possible to identify recent trends in intermediary liability policy.

Since the enactment of the first safe harbours and liability exemptions for online intermediaries, market conditions have radically changed. Originally, intermediary liability exemptions were introduced to promote an emerging Internet market. Do safe harbours for online intermediaries still serve innovation? Should they be limited or expanded? Such critical questions—often tainted by protectionist concerns—define the present intermediary liability conundrum. Apparently, safe harbours still hold importance, although secondary liability for illegal content online is on the rise.

Besides a consistent enforcement of online intermediaries' safe harbors in the United States,[48] several emerging economies have been bringing their legal system up to digital speed. Recently, the Brazilian Marco Civil da Internet—or Internet Bill of Rights—introduced a civil liability exemption for Internet access providers and other Internet providers.[49] n the case of hosting providers, Article 19 provides that, "*in order to ensure freedom of expression and to prevent censorship, an Internet application provider shall only be subject to civil liability for damages caused by virtue of content generated by third parties if, after specific court order, it does not take action [. . .] to make the infringing content unavailable*."[50] This broad civil—and

[48] However, the United States Copyright Office is undertaking a public study to evaluate the impact and effectiveness of the safe harbour provisions. In particular, notice-and-stay-down arrangements—rather than takedown—are under review in the United States as well as elsewhere. *See* United States Copyright Office, Section 512 Study, http://copyright.gov/policy/section512; *see also* BMG Rights Management (US) LLC *et al* v. Cox Enterprises, Inc. *et al*, 1:14-cv-1611 (August 9, 2016) (confirming a jury verdict of December 2015 holding that Cox—the broadband provider—forfeited the immunity of the Digital Millennium Copyright Act, 1998 by not blocking music piracy by its subscribers after BMG had alerted Cox to the wrongdoing of individual infringers identified by Rightscorp, a provider of litigation services against copyright infringers).

[49] *See* Marco Civil da Federal Law no. 12.965, April 23, 2014, Art. 18, *available at* https://cyberlaw.stanford.edu/page/wilmap-brazil ("the Internet connection [*access*] provider shall not be subject to civil liability for content generated by third party").

[50] *Id*., at Art. 19.

not criminal—liability exemption, however, does not apply to copyright infringement.[51] Other African, Asian and South American countries have also been discussing the introduction of a safe harbour regime for quite some time now. The Hong Kong government, for example, introduced a copyright bill establishing a statutory safe harbour for OSPs for copyright infringement, provided that the OSPs meet certain prescribed conditions, including the taking of reasonable steps to limit or stop copyright infringement upon being notified.[52]

Nonetheless, safe harbours' recalibration towards greater secondary liability for online intermediaries does characterize the recent international policy debate. Increasing number of cracks are appearing in safe harbour arrangements for online intermediaries. Increased intermediary accountability has become a global trend that has been emerging in Europe, Asia, South America, Africa and Australia.

As anticipated, voluntary and private censorship of allegedly illegal online content—shifting the discourse from intermediary liability to intermediary responsibility or accountability—is a core policy trend. Voluntary measures—which the European Commission would like to promote among platforms—do shake the EU intermediary liability system. Hosting providers—especially platforms—would be called to actively and swiftly remove illegal materials, instead of reacting to complaints. The OP&DSM Communication puts forward the idea that 'the responsibility of online platforms is a key and cross-cutting issue.'[53] In other words, intermediary liability expansion—and limitation of safe harbors—will occur by imposing an obligation on online platforms to behave responsibly by addressing specific problems. The European Commission aligns its strategy for online platforms to a globalized, ongoing move towards privatization of law enforcement

---

[51] *Id*., at Art. 19 (2).

[52] *See* Copyright Amendment Bill, 2014, C2957, Clause 50, *available at* http://www.gld.gov.hk/egazette/pdf/20141824/es32014182421.pdf; *see also* Bolin Zhang, Hong Kong Government Introduces Copyright Bill Providing a "Safe Harbour" for OSPs for Copyright Infringement, CIS Blog, June 17, 2014, https://cyberlaw.stanford.edu/blog/2014/06/hong-kong-government-introduces-copyright-bill-providing-%E2%80%9Csafe-harbor%E2%80%9D-osps-copyright (noting that the safe harbour will be underpinned by a Code of Practice which sets out practical guidelines and procedures for OSPs to follow upon notification of infringement such as "notice-and-notice" and "notice-and-takedown.").

[53] Communication from the Commission of the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM (2016) 288 Final, at 9 (May 25, 2016) [hereinafter, "OP&DMS Communication"] *available at*https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe.

online through algorithmic tools.[54] Coordinated EU-wide self-regulatory efforts by online platforms should immediately be directed to fight incitement to terrorism and to prevent cyber-bullying.[55] In fact, as an immediate result of this new policy trend, the European 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 speech online in Europe.[56] 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.[57] Some EU member States, such as Germany, may even bring in a law to impose fines of up to €500,000 on a platform failing to take down illegal content within 24 hours.[58]

On the intellectual property enforcement side, payment blockades—notice-and-termination agreement between major right holders and online payment processors—and "*voluntary best practices agreements*" for copyright and trademark enforcement have been applied widely, especially in the United States.[59] 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.[60] In the Communication *Towards a Modern, More European Copyright Framework*, the European Commission would like to

---

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

[55] *See* OP&DMS Communication, *supra* note 53, at 10.

[56] *See* Commission, European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech, Press Release (May 31, 2016), http://europa.eu/rapid/press-release_IP-16-1937_en.htm; European Commission, Justice and Consumers, Fighting Illegal Online Hate Speech: First Assessment of the New Code of Conduct, Press Release (December 12, 2016), http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50840 (urging platforms to do more to implement the Code of Conduct).

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

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

[59] *See* Annemarie Bridy, *Internet Payment Blockades*, 67 Florida L. Rev. 1523 (2015); *see also* Derek E. Bambauer, *Against Jawboning*, 100 Minnesota L. Rev. 51 (2015) (discussing federal and state governments' increasing regulation of online content through informal enforcement measures, such as threats, at the edge of or outside their authority).

[60] *See* Bridy, *supra* note 59, at 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).

endorse similar strategies by deploying a 'follow-the-money' approach.[61] 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'.[62] According to the Commission, 'follow-the-money' mechanism should be based on a self-regulatory approach through the implementation of Code of Conducts that might be later backed up by legislation if necessary.

As part of its Digital Single Market Strategy, the European Commission has been seriously considering for some time now to narrow the eCommerce Directive horizontal liability limitations for Internet intermediaries[63] and putting in place a "*fit for purpose*"—or vertical—regulatory environment for platforms and intermediaries.[64] It is planning to introduce enhanced obligations on websites and other Internet intermediaries for dealing with unlawful third-party content.[65] In particular, the Commission is discussing what regulations should apply to a subset of the intermediaries deemed as "*online platforms*" and "*whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems—a duty of care*"[66] with the aim to achieve a fairer allocation of

---

[61] *See* Communication from the Commission of the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Towards a Modern More European Copyright Framework, COM (2015) 260 Final, at 10-11 (December 9, 2015).

[62] *Ibid*.

[63] *See* Patrick Van Eecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, 48(5) Common Market L. Rev. 1455, 1463 (2011) (noting that "Section 4 [of the eCommerce Directive] introduces a horizontal special liability regime for the three types of service providers covered by it. Provided they meet the criteria laid down in Section 4, the service providers will be exempted from contractual liability, administrative liability, tortious/extra-contractual liability, penal liability, civil liability or any other type of liability, for all types of activities initiated by third parties, including copyright and trademark infringements, defamation, misleading advertising, unfair commercial practices, unfair competition, publications of illegal content, etc.").

[64] *See* European Commission, Communication, A Digital Single Market Strategy for Europe, COM (2015) 192 Final, May 6, 2015, at § 3.3, *available at* http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf [hereinafter, "Digital Single Market Strategy"]; *see also* for a general overview of the intermediary liability framework in Europe, Christina Angelopoulos, European Intermediary Liability in Copyright: A Tort-Based Analysis (Kluwer Law Int'l 2016).

[65] Digital Single Market Strategy, at 3.3.2 (noting that "[r]ecent events have added to the public debate on whether to enhance the overall level of protection from illegal material on the Internet.").

[66] *Id*.; *see also* eCommerce Directive, *supra* note 37, at 48, (previously establishing that "[t]his Directive does not affect the possibility for member States of requiring service providers, who host information provided by recipients of their service, to *apply duties of care*, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities") (emphasis added).

value generated by the distribution of copyright-protected content by online platforms.[67] The Commission presented this platform-sensitive update of the EU copyright policy in a proposal for a Directive on Copyright in the Digital Single Market,[68] which is part of a larger package aiming at modernizing the EU copyright rules and achieving a fully functioning Digital Single Market.[69] A groundbreaking provision aiming at closing the "*value gap*"—and closely affecting online intermediaries—is the introduction of an ancillary right for the reproduction of press publications in respect of digital uses and ensuring their availability for the public.[70] The proposed reform also includes a second provision that would broadly impact platform operations in order to close the so-called "*value gap*". It requires intermediaries "*that store and provide access to large amounts of works [. . .] uploaded by their users*" to take appropriate and proportionate "*measures to ensure the functioning of agreements concluded with rightholders for the use of their works*" or "*to prevent the availability on their services of [such] works*," including through "*the use of effective content identification technologies*."[71]

Meanwhile, some member States have already taken the regulatory path or are in the process of doing so. The German coalition agreement included the prospect of expanded hosting provider liability for online copyright infringement.[72] In 2013, Germany amended its Copyright Law by providing exclusive neighbouring rights to press publishers. The new right covers ensuring availability of any publications and their fragments, beyond individual words and the smallest text excerpt, for commercial purpose.[73] Further, a recent Spanish copyright reform expanded intermediary liability by introducing, *inter alia*, doctrines of secondary liability—inducement, contributory and vicarious liability—in the Spanish legal system.[74] In addition—following the footsteps of the German amendment—the Spanish

---

[67] *See* OP&DMS Communication, *supra* note 53, at 8.

[68] Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, COM (2016) 593 Final (September 14, 2016), Art. 13 [hereinafter, "DSM Directive Proposal"].

[69] *See* European Commission, Digital Single Market, Modernization of the EU Copyright Rules, http://bit.ly/DSMCopyright16.

[70] *See* DSM Directive Proposal, *supra* note 68, at Art. 13, at 11(1).

[71] *See* DSM Directive Proposal, *supra* note 68, at Art. 13(1).

[72] *See* Deutschlands Zukunft Gestalten – Koalitionsvertrag Zwischen CDU, CSU und SPD, 18 Legislaturperiode (December 17, 2013), at 133-134, *available at* https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf [hereinafter, "German Coalition Agreement"].

[73] *See* Articles 87f-87h of the German Law on Authors' and Neighbouring Rights.

[74] *See* Real Decreto Legislativo (RDL) 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, BOE-A-1996-8930, Art. 138, as amended by Ley 21/2014, de 4 de noviembre, BOE-A-2014-11404, *available at* https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930&tn=1&p=20141105 &vd=#a32.

reform created a highly controversial compulsory levy for news aggregators.[75] Also known as "*Google tax*," the Spanish reform lead Google to terminate its Google News service in Spain.

The recent EU reform proposal would force hosting providers to develop and deploy filtering systems, therefore, *de facto* monitoring their networks.[76] This proposal follows in the footsteps of a well-established path in recent intermediary liability policy: the demise of the principle of "*no monitoring obligations*". In the same vein, recent case law has imposed proactive monitor obligations on intermediaries for copyright infringement—such as Allostreaming in France, Dafra in Brazil, RapidShare in Germany, or Baidu in China.[77] In fact, the emerging enforcement of proactive monitoring obligations spans the entire spectrum of intermediary liability subject matters: other intellectual property,[78] privacy,[79] defamation, and hate/dangerous speech.[80] In this context, notable exceptions—such as the landmark Belen

---

[75] *Id*., at Art 32(2).

[76] *See* DSM Directive Proposal, *supra* note 68, at Recital 38-39 and Art. 13(1).

[77] *See* APC et al v. Google, Microsoft, Yahoo!, Bouygues et al (TGI Paris, 2013) (France), *available at* http://cyberlaw.stanford.edu/page/wilmap-france(imposing an obligation on search engines 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, March 24, 2014) (Brazil), *available at* https://cyberlaw.stanford.edu/page/wilmap-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), *available at* https://cyberlaw.stanford.edu/page/wilmap-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), *available at* https://cyberlaw.stanford.edu/page/wilmap-china (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).

[78] Rolex v. eBay (a.k.a. *Internetversteigerung* II), I ZR 35/04 (BGH, April 19, 2007) (Germany); Rolex v. Ricardo (a.k.a. *Internetversteigerung*III), Case I ZR 73/05, (BGH, April 30, 2008) (Germany) (in the so-called Internet Auction cases I-III, the German Federal Court of Justice—*Bundesgerichtshof*—repeatedly decided that notified trademark infringements oblige internet auction platforms such as eBay to investigate future offerings—manually or through software filters—in order to avoid trademark infringement).

[79] *See* Google v. Mosley (TGI Paris, November 6, 2013) (France), *available at* http://cyberlaw.stanford.edu/page/wilmap-france; Max Mosley v. Google Inc., 324 O 264/11 (Hamburg District Court, January 24, 2014), *available at* http://openjur.de/u/674344.html; Mosley v. Google, 2015 EWHC 59 (QB) (United Kingdom), *available at* http://cyberlaw.stanford.edu/page/wilmap-united-kingdom (courts in France, Germany, and the UK imposing proactive monitoring obligations on 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 having sex with prostitutes wearing Nazi paraphernalia).

[80] Delfi AS v. Estonia No 64569/09 (ECtHR, June 16, 2015), *available at* http://hudoc.echr.coe.int/eng?i=001-155105 (finding complaint with ECHR a decision imposing monitoring obligation on a news web portal for defamatory users' comments).

case in Argentina—also highlight a fragmented international response to intermediary liability.[81]

Another relevant trend in intermediary liability is the blocking orders against innocent third parties. Blocking orders have become increasingly popular in Europe, especially to contrast online copyright—and recently also trademark—infringement.[82] Their validity under EU law was recently confirmed by the European Court of Justice in the Telekabel decision.[83] Outside the EU, website blocking of copyright infringing sites has been authorised in countries including Argentina, India, Indonesia, Malaysia, Mexico, South Korea and Turkey.[84] In December 2014, Singapore effected an amendment to its Copyright Act to enable right holders to obtain website blocking orders,[85] and in 2015, Australia introduced "*website blocking*" provisions to its Copyright Act.[86] These measures have been enacted to curb intellectual property infringement online. However, negative effects of these measures on human rights have also been widely highlighted.[87]

Regardless, blocking orders have been widely used in multiple jurisdictions—in particular by administrative authorities—in connection with

---

[81] *See* Rodriguez M. Belen v. Google, R.522.XLIX. (Supreme Court, October 29, 2014 (Argentina), (rejecting 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, honor and privacy), *available at* https://cyberlaw.stanford.edu/page/wilmap-argentina.

[82] *See* Directive 2004/48/EC on the Enforcement of Intellectual Property Rights, Art. 11; Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Art. 8(3); *see also* for an overview of European caselaw, Giancarlo Frosio, Alalalai!... Rojadirecta is Up for Battle Again in Italy, CIS Blog (September 6, 2013), http://cyberlaw.stanford.edu/blog/2013/09/alalalai-rojadirecta-battle-again-italy; Giancarlo Frosio, UK High Court Orders ISPs to Block IP Address, Erroneously Takes Down Hundreds of Sites, CIS Blog (September 22, 2013), https://cyberlaw.stanford.edu/blog/2013/09/uk-high-court-orders-isps-block-ip-address-erroneously-takes-down-hundreds-sites; Giancarlo Frosio, Cartier v. BSkyB: UK Judge Orders ISPs to Block Websites Infringing Trademarks for the First Time in Europe, CIS Blog (November 7, 2014), http://cyberlaw.stanford.edu/blog/2014/11/cartier-vs-bskyb-uk-judge-orders-isps-block-websites-infringing-trademarks-first-time.

[83] *See* UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 Bus LR 541.

[84] *See* Council of Europe, Filtering, Blocking and Take-down of Illegal Content of the Internet (a study commissioned to the Swiss Institute of Comparative Law), http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.

[85] *See* Copyright (Amendment) Act, 2014, An Act to Amend the Copyright Act (Chapter 63 of the 2006 Revised Edition), available at http://cyberlaw.stanford.edu/page/wilmap-singapore.

[86] *See* Copyright Amendment (Online Infringement) Act, 2015 (Cth), *available at* http://cyberlaw.stanford.edu/page/wilmap-australia.

[87] *See* Christophe Geiger and Elena Izyumenko, *The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking*, 32(1) American U. Int'l L. Rev. 43 (2016).

amorphous notions of public order, defamation, and morality. In this respect, the emergence of administrative enforcement of online intermediary liability appears as another well-marked trend in recent Internet governance. Multiple administrative bodies have been put in charge of enforcing a miscellaneous array of online infringements—primarily against intermediaries—and judicial supervision is often absent in these cases. Some administrative bodies—such as the Italian Communication Authority (AGCOM) and Second Section of the Copyright Commission (CPI)—have been provided with powers to police copyright infringement online and issue blocking orders and other decisions to selectively remove infringing digital works.[88]

Many other administrative agencies enjoy broader powers of sanitization of the Internet. The Russian Roskomnadzor is an administrative body competent to request telecom operators to block access to websites featuring content that violates miscellaneous pieces of legislation. It is also competent to keep a special registry or "*blacklist*" where it adds websites that violate the law.[89] In South Korea, Korea Communications Commission implements deletion or blocking orders according to the requests and standards of the Korea Communications Standards Commission "*as necessary for nurturing sound communications ethics*."[90] In Turkey, the law empowers the Presidency of Telecommunications (TIB) to block a website or web page within 4 hours without any judicial decision for the violation of a new category of crimes labelled as "*violation of private life*" or privacy.[91] Similarly, in India, Section 69A(1) of the Information Technology Act, 2000 provides the government with the "*power to issue directions for blocking for public access of any information through any computer resource*".[92] This is

---

[88] *See* AGCOM Regulations regarding Online Copyright Enforcement, 680/13/CONS, December 12, 2013, *available at* http://cyberlaw.stanford.edu/page/wilmap-italy; Royal Legislative Decree No. 1/1996, enacting the consolidated text of the Copyright Act, April 12, 1996 (as amended by the Law No. 21/2014, November 4, 2014), *available at* http://cyberlaw.stanford.edu/page/wilmap-spain.

[89] *See* 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"), July 28, 2012, *available at* http://cyberlaw.stanford.edu/page/wilmap-russia.

[90] *See* Act on the Establishment and Operation of Korea Communications Commission (KCCA), last amended by Act No. 11711, March 23, 2013, *available at* http://cyberlaw.stanford.edu/page/wilmap-south-korea.

[91] *See* 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, *available at* http://cyberlaw.stanford.edu/page/wilmap-turkey.

[92] *See* Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act 2008, Section 69A(1), *available at* http://cyberlaw.stanford.edu/page/wilmap-india.

dealt with by a special Committee which examines within seven days all the requests received for blocking access to online information according to Section 69A(1).[93] In *Shreya Singhal* v. *Union of India*, the Supreme Court of India confirmed the validity of blocking orders issued under Section 69 of the Information Technology Act, 2000, although under certain limitations.[94] Many other national administrative authorities—such as the Supreme Council of Cyberspace in Iran or CONATEL in Venezuela—also issue orders against Internet Service Providers (ISPs) regarding the legality, blocking and removal of online content, which do not involve—or involve very limited—judicial review.[95] Concerned views have been voiced against administratively issued blocking orders, on grounds of undermining of the guarantee of basic due process. In particular, such orders run counter to the second Manila Intermediary Liability Principle, which states that content must not be required to be restricted without an order by a judicial authority.[96]

In the information society, the role of private sector entities in gathering information for and about users has long been a very critical issue. Therefore, intermediaries have become a main focus of privacy regulations, especially in jurisdictions such as Europe which have a strong tradition of privacy protection.[97] In a landmark case of Google Spain, the European Court of Justice ruled that an internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties.[98] Multiple jurisdictions are trying to

---

[93] *See* Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (to be read with Section 69A of the Information Technology Act, 2000), Rule 7, *available at* http://cyberlaw.stanford.edu/page/wilmap-india.

[94] *See* Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[95] *See* Executive Order of the Supreme Leader Establishing the Supreme Council of Cyberspace, March 2012, *available at* http://cyberlaw.stanford.edu/page/wilmap-iran; Ley de Responsabilidad Social en Radio Televisión y Medios Electrónicos [ResorteME] [Law of Social Responsibility in Radio-Television and Electronic Media], Official Gazette No. 39.579, December 22, 2012, *available at* http://cyberlaw.stanford.edu/page/wilmap-venezuela.

[96] *See* Manila Principles, *supra* note 16, at Principle No. 2.

[97] *See* Bart van der Sloot, Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe, 6 JIPITEC 211 (2015).

[98] *See* Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 QB 1022 : (2014) 3 WLR 659, *available at* https://cyberlaw.stanford.edu/page/wilmap-european-union; *see also* (clarifying that (1) Search engines qualify as data controllers under Directive 95/46/EC to a search engine insofar as (a) the processing of personal data is carried out in the context of the activities of a subsidiary on the territory of a Member State, (b) set up to promote and sell advertising space on its search engine in this member State with the aim of making that service profitable. In this case, the processing of data by search engines, "must be distinguished from, and is additional to that carried out by publishers of third-party websites"); Christopher Kuner, *The Court of Justice of the EU Judgment on*

cope with RTBF demands following this landmark case.[99] The emergence of the RTBF—and its extra-territorial application which will be mentioned later—follows in the footsteps of a global move towards data protectionism against the *de facto* market dominance of the United States Internet conglomerates.[100] There are plenty of recent examples, including the European Court of Justice's *Schrems* decision and the Russian Federal Law No. 242-FZ. In *Schrems*, the European Court of Justice had ruled that the transatlantic Safe Harbor Agreement—which lets American companies use a single standard for consumer privacy and data storage in both the United States and Europe—is invalid.[101] Russia also introduced a legislation that requires that the processing of personal data of Russian citizens be conducted with the use of servers located in Russia.[102]

Finally, extra-territorial enforcement of intermediaries' obligations might be the next emerging trend in intermediary liability policy. This phenomenon is closely attached to the protectionist impulses that characterize present international relationships and Internet governance. Extra-territorial enforcement recently made the headlines for the worldwide enforcement of the RTBF. European institutions endorse the view that delisting should have an extra-territorial reach. On the territorial effect of de-listing decisions, the WP29 Guidelines noted that limiting de-listing to EU domains cannot be considered as a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, "*this means that in any*

Data Protection and Internet Search Engines: Current Issues and Future Challenges, *in* Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55 (Burkhard Hess and Cristina M. Mariottini (eds.), Ashgate 2015), *available at* http://ssrn.com/abstract=2496060.

[99] *See* Giancarlo F. Frosio, *Right to be Forgotten: Much Ado About Nothing*, 15(2) Colorado Tech. L. J. (forthcoming 2017), *available at* https://ssrn.com/abstract=2908993.

[100] *See* Maria Farrel, 'How the Rest of the World Feels About U.S. Dominance of the Internet' (Slate, November 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/11/the_u_s_should_stop_lecturing_about_internet_values.html.

[101] *See*, *e.g.*, Schrems v. Data Protection Commr., 2016 QB 527 : (2016) 2 WLR 873.

[102] *See* Federal Law No. 242-FZ, on Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks, July 21, 2014, *available at* http://cyberlaw.stanford.edu/page/wilmap-russia; *see also* CNiL, The French Data Protection Authority Publicly Issues Formal Notice to Facebook to Comply with the French Data Protection Act within Three Months, February 9, 2016, https://w ww.cnil.fr/en/french-data-protection-authority-publicly-issues-formal-notice-facebook-comply-french-data; Felipe Busnello and Giancarlo Frosio, WhatsApp in Brazil?, CIS Blog, December 28, 2015, https://cyberlaw.stanford.edu/blog/2015/12/whatsapp-brazil; Mark Scott, 'Russia Prepares to Block LinkedIn After Court Ruling'(The New York Times, November 10, 2016), http://www.nytimes.com/2016/11/11/technology/russia-linkedin-data-court-blocked.html (as LinkedIn does not comply with recent legal obligations in Russia that require all companies doing business in the country to store their data locally).

case de-listing should also be effective on all relevant .com domains."[103] Recently—in accordance with the WP29 Guidelines—the Commission Nationale de l'informatiqueet des Libertés (CNiL), the French data protection authority—ordered Google to apply the RTBF on all domain names of Google's search engine, including the .com domain.[104] Meanwhile, decisions imposing extra-territorial obligations on intermediaries have appeared elsewhere too. The Court of Appeal of British Columbia issued an order requiring Google to remove websites from its worldwide index. The court order—which is now under review with the Supreme Court of Canada—is unprecedented for Canada as it forces Google to remove links anywhere in the world, rather than only from the search results available through Google.ca.[105] While extra-territorial enforcement might potentially break the Internet, it is telling of a disconnection between physical and digital governance of information and content, and this disconnection seems to be unwilling to go away, at least for some time.

VI. Conclusions

Given the online intermediaries' role in the digital interconnected society, their liability for the speech and content they carry has become a primary policy concern. Much has changed since the inception of the first online intermediary and its regulation. New challenges have brought to forea discussion regarding the scope of intermediaries' duties and obligations. The WILMap has been developed to promote better understanding of a confusing international legal framework. Several other projects in the last few years have also aimed at reducing uncertainty regarding the international intermediary liability conundrum online. This uncertainty can hurt users by potentially scaring companies away from providing innovative new services in certain markets. Additionally, companies may unnecessarily limit what users can do online, or engage in censorship-by-proxy to avoid uncertain retribution under unfamiliar laws. National courts and authorities, on the other hand, may seek extra-territorial enforcement to prevent any access to

[103] Art. 29 Data Protection Working Party, Guidelines to the Implementation of the CJEU Judgment on Google Spain v. Costeja, 14/EN WP 225 (November 26, 2014), at 3 (emphasis added).

[104] *See* CNiL, Restricted Committee, Deliberation No. 2016-054 (March 10, 2016), https://www.cnil.fr/sites/default/files/atoms/files/d2016-054_penalty_google.pdf; *see also* CNiL Orders Google to Apply Delisting on all Domain Names of the Search Engine, CNiL, June 12, 2015, https://www.cnil.fr/fr/node/15790.

[105] *See* Equustek Solutions Inc. v. Google Inc., 2015 BCCA 265 (Court of Appeal of British Columbia 2015), *available at* http://www.courts.gov.bc.ca/jdb-txt/CA/15/02/2015BCCA0265.htm.

infringing materials in their jurisdiction. As a result, in such a confusing legal and theoretical landscape, there is a growing tendency towards Internet fragmentation, which is made even more obvious by unconcealed national tendencies toward data protectionism.

Further, as discussed, the intermediary liability discourse is shifting towards an intermediary responsibility discourse. This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention to police allegedly infringing activities on the Internet. Several emerging legal trends in the intermediary liability domain reflect this change in perspectives, such as voluntary agreements and private enforcement. This is also reflected by other legal arrangements that make the role of online intermediaries more prominent. This is the case of three-strike legislations, blocking orders dealt almost entirely between intermediaries and rightholders, and administrative enforcement of intermediary liability online. Meanwhile, retraction of intermediaries' safe harbours, proactive monitoring obligations, and the wider enforcement of blocking orders further accomplish the goal of turning online intermediaries into Internet police.