Zingales, Nicolo

Conference Paper

The Brazilian Approach to Internet Intermediary Liability: Blueprint for a Global Regime?

20th Biennial Conference of the International Telecommunications Society (ITS): "The Net and the Internet - Emerging Markets and Policies" , Rio de Janeiro, Brazil, 30th-03rd December, 2014

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Zingales, Nicolo (2014) : The Brazilian Approach to Internet Intermediary Liability: Blueprint for a Global Regime?, 20th Biennial Conference of the International Telecommunications Society (ITS): "The Net and the Internet - Emerging Markets and Policies" , Rio de Janeiro, Brazil, 30th-03rd December, 2014, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/106847

THE BRAZILIAN APPROACH TO INTERNET INTERMEDIARY LIABILITY: BLUEPRINT FOR A GLOBAL REGIME?

Nicolo Zingales*

Introduction

One of the most critical Internet governance issues of our time is the definition of an adequate framework on the responsibility of intermediaries for user-generated content. Internet intermediary liability is a wide-ranging topic, stretching into many different areas of law, from defamation and privacy to trademark and copyright infringement. Given the substantial difference between the issues at stake in these areas, legislators in many countries adopted domain-specific solutions, with the aim to appropriately account for the tension between different rights and interests at stake. In an increasingly interdependent digital environment, with an Internet dominated by multinational corporations providing their services across the entire world, this heterogeneity generates significant problems of compliance and friction across different regimes. The controversial stand taken by the European Union in recognizing a so called "right to be forgotten"[1], seen together with the reactions by US legal scholars[2] and the proposals for the adoption of a similar right currently under consideration in Brazil[3], Japan[4] and Korea[5], offers one notable example

* Assistant professor, Tilburg Law School, Tilburg Law and Economics Center; Fellow, Center for Technology and Society, Fundacao Getulio Vargas. Preliminary draft, presented at the International Telecommunication Society Biennial Conference ("The Net and the Internet: Emerging Market and Policies", 30 November- 2 December 2014). Comments welcome at n.zingales@uvt.nl

[1] See the proposed EU Data Protection Regulation, available at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (in particular, art. 17); and the judgement of the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos* (AEPD), Case C- 131/12 (E.C.R. May 13, 2014)

[2] See Jonathan Zittrain, "Is the EU compelling Google to become about.me?" The Future of the Internet and How to Stop It (May 13th, 2014), available at http://blogs.law.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/ ; " Don't force Google to Forget", New York Times (May 14th, 2014), available at http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0; Monkey Cage, "Five Key Questions about the European Court of Justice's Google decision", Washington Post (May 14th, 2014); hhttp://www.washingtonpost.com/blogs/monkey-cage/wp/2014/05/14/five-key-questions-about-the-european-court-of-justices-google-decision/?wprss=rss_politics;
Annemarie Bridy, "Google Spain and the Right to Be Forgotten", Freedom to Tinker (May 14th, 2014) available at https://freedom-to-tinker.com/blog/abridy/google-spain-and-the-right-to-be-forgotten/ Henry Farrell and Abraham Newman, "Forget me not", Foreign Affairs (May 15th, 2014), available at http://www.foreignaffairs.com/articles/141435/henry-farrell-and-abraham-newman/forget-me-not; Meg Leta Ambrose, "EU Right to be Forgotten Case: The Honorable Google Handed Both Burden", Plagiarizing for Educational Purpose (May 19th, 2014), available at http://playgiarizing.com/2014/05/19/eu-right-to-be-forgotten-case-the-honorable-google-handed-both-burden-and-boon/

[3] See Bill N. 7781/2014, of Mr. Renato Cunha; available at http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1270760&filename=PL+7881/2014; and explained in English at "Brazilian Congressman Introduces Right to Be Forgotten Bill", Information Security Blog (October 23th, 2014) , available at https://www.huntonprivacyblog.com/2014/10/articles/brazilian-congressman-introduces-right-forgotten-bill/

of such friction. Differences of cultures, approaches and underlying values are exposed, rather than mediated, in the absence of a dedicated global governance forum defining guiding principles for the involvement of Internet intermediaries in the enforcement of rights of their users. This paper aims to set the seeds for the creation of such global mechanism, and suggests that the model chosen by Brazil in its recent civil framework for the Internet (Marco Civil da Internet) can be used as an inspiration to frame this discussion.

Section I briefly illustrates the clashes of interests that underlie the discussions on intermediary liability, including distinctions of the role of such parties under different scenarios. Section 2 then defines conceptually the notion of intermediaries, highlighting some of the open definitional questions; and Section 3 goes into more detail addressing the specific definitions given in the context of US and EU legislation, as testament to the wide divergence between the existing approaches. Section 4 describes the remarkable achievements of the Brazilian Marco Civil, signed into law in April 2014, and explains the tensions underlying some of its key provisions. Section 5 situates the novelty of the Brazilian approach into a taxonomy of intermediary liability regimes, taking stock and reflecting on what interests are best served by each of these regimes. Finally, Section 6 purports to define the foundations for a "global Marco Civil" by identifying key principles deriving from international human rights law, and advances the idea of a global forum for the discussion of the implementation of such principles into intermediary liability provisions.

1. The dilemma of Internet intermediary liability: exposing the clashes of interests

At its basic, Internet intermediary liability is concerned with one fundamental question: what are reasonable normative expectations of involvement by intermediaries in the enforcement of different laws and regulations? If on one hand, the protection of rights in cyberspace may be deprived of its effectiveness without the ability to rely on intermediaries for immediate enforcement, on the other hand imposing on intermediaries the duty to monitor the activity of their customers and/or prevent the publication of any potentially infringing content constitutes a serious restraint on speech, which should only be permitted under stringent conditions in international human rights law [6]. Moreover, imposing a duty to monitor or police content leads to the risk of having the intermediary holding back the emergence of new services with even the slightest potential of infringing content, and generates a "culture of permission" which is ill-suited for the development of innovative products and services in the information society. Accordingly, while strict intermediary liability provisions can be a boon to content

[4] See Tomoko Otake, "Right to be forgotten' on the Internet gains traction in Japan". (December 9th, 2014). Available at http://www.japantimes.co.jp/news/2014/12/09/national/crime-legal/right-to-be-forgotten-on-the-internet-gains-traction-in-japan/#.VR18elbov8E

[5] Sooyoung Oh, "The Right to Be Forgotten in Korea" (August 19th, 2014). Available at http://www.humanrightskorea.org/2014/right-to-be-forgotten-korea/

[6] For example, according to international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) and regional human rights conventions, a number of restrictions must be necessary for the attainment of an objective that has been clearly recognized and disciplined by law. See e.g. article 12, 14, 19, 21 and 23 of the ICCPR.

creators under the established model of knowledge production and distribution, they have a potentially devastating effect on disruptive or even moderately innovative forms of knowledge creation, to the extent that the intermediary can be found responsible both for the content generated by its user(s), and for the activity performed by itself in enabling such content to reach its audience.

To obviate these concerns, legal systems generally define some "comfort zones", also known as "safe harbours", where intermediaries can operate without being held responsible for the conduct of their users. However, these safe harbours are of different scopes and different degrees, thereby generating conflicting standards which are at odds with the transnational nature of the Internet. Besides the conceptual challenges on the definition of Internet intermediaries, a practical challenge concerns the design of the regime that is chosen to determine their rules of behavior. Quite logically, whether a standard is fit for purpose will depend on whose perspective one adopts. For this reason, understanding the actors, their needs and their concerns with different regimes is crucial to the formulation of the appropriate rules.

While a divergence of interests is evident between content producers and infrastructure providers, who aspire being treated as "dumb pipes" who are not expected to either detect or remove potentially illegal material, less visible or widely known are the tension within these two categories: for example, big content producers place great importance on the involvement of intermediaries, while small and independent producers –particularly if they produce some kind of transformative work- have an interest in fostering a culture of "no permission", which is hard to reconcile with the idea of an intermediary monitoring content- and particularly so with the rise of automated, quick and effective enforcement mechanisms. Similarly, within the infrastructure providers one can distinguish mere conduits from those who provide more advanced or additional services: even where such specification falls short of content production, their interests are better served by a regime which does not rely excessively on their role in detecting and removing potentially infringing material.

This is however slightly different with regard to privacy and defamation, where there is a certain degree of alignment of interests, across sectors, in considering that infrastructure providers should not be encouraged to preventively remove content in the belief that such content might be infringing of the right of an individual to control the information of him or her that is available on the Internet[7]. Even there, a difference might exist in the public character of a particular figure or situation, as it raises concerns of public right to know that ought to be balanced against possible claims of control over that information. This does not suggest in itself that the intermediary should not be involved in the enforcement simply because it cannot make such judgments appropriately, but it does pose the question of the extent to which the balancing called upon in this context should rather be left to courts.

[7] An exception to this trend is the Delfi case, where the Supreme Court of Estonia established that a news portal was liable for having, *inter alia*, and inadequate system of filtering of potentially defamatory content; see *Delfi v. Estonia*, Judgment of the ECtHR on 10 October 2013 (Application no. 64569/09), pending before the Grand Chamber.

In fact, despite differences in the type and weight of the interests involved, these areas are aligned with intellectual property in being best served by a regime where judicial authorities are involved before the adoption of any significant decision, precisely in recognition of the complexity of the assessment that needs to be undertaken. At the other extreme lie strong public policy interests, such as the fight against child pornography and the prevention of malware, in which there is almost unanimous consensus of the need for a proactive involvement of intermediaries. Here, the clash of interest within the group is minimal, as the only constituency opposing such type of engagement would be composed by those producing legal material who may potentially be seen as falling under one of those categories. Note that the intra-group conflict (i.e. between infrastructure and content providers/viewers) remains significant; however, the strength of the public policy interest here weighs heavily against the limitation of liability of infrastructure providers in this context.

Another important point with regard to copyright is that the interests of Internet service providers are often in direct tension with those of copyright owners when it comes to the definition of the specific rules of intermediary liability, therefore making a consensus more difficult to reach in this particular context. This difficulty can be ascertained, for example, in the failure of the long process of negotiation which followed the approval of the Digital Economy Act (in 2010) in the U.K., where the communication regulator (OFCOM) was assigned with the task to implement general principles by brokering a multistakeholder consensus on the splitting of costs for the filtering imposed to ISPs in order to prevent copyright infringement[8]. While extensive discussions were , on May 9th, 2014, the BBC revealed that an agreement on voluntary (including technical) measures of protection had been achieved privately between ISPs and copyright owners[9], bypassing the very multistakeholder nature of the regulation that the Act intended to achieve with the consultation. While the failure of the institutional mechanism seems to be due the attempt to reach multistakeholder consensus in an area of inherent conflict between ISPs and copyright industry, the importance of copyright enforcement in the discussions of intermediary liability should not be underestimated. This suggests that its separation from other areas of intermediary liability might facilitate decision-making, allowing for a balance to be struck between multiple diffuse interests, rather than at the whim of the few, resourceful and well organized who manage to meaningfully participate in the decision-making process. Before we substantiate this claim, however, it is important to understand what exactly are the subjects of this analysis: Internet intermediaries.

2. The common ground: defining "intermediaries"

A widely accepted starting point is that a service provider can be qualified as such if it is directly involved in processing the information generated by the user. However, legal systems differ as to the extent to which such involvement can be ascribed to merely

[8] See Online Infringement of Copyright and the Digital Economy Act 2010, and "Notice of Ofcom's proposal to make by order a code for regulating the initial obligations", available at http://stakeholders.ofcom.org.uk/consultations/infringement-notice/summary

[9] Dave Lee, "Deal to combat piracy in UK with 'alerts' is imminent", BBC news (May 9th, 2014); available at http://www.bbc.com/news/technology-27330150

"passive" providers, such as ISPs and network operators. There is also no consensus on the potential reach of the definition with regard to products (as opposed to services), such as those of software developers and hardware manufacturers (including those specialized in filtering technologies).

A dictionary definition of intermediaries sees them as entities functioning as means of communication between different actors helping them to make an agreement [10]. In the context of the Internet however, this definition needs to be adjusted to refer to the provision of services that enable Internet communication between different users. A proper definition must on the one hand recognize the ongoing character of the activity that is offered to Internet users (be it via a long-term contract or one-off transactions), so as to enable global networked communications; on the other hand, it must account for the fact that the ultimate action that is sought after by the customers of these intermediaries is the accomplishment of a communicative act, as it enables them to connect to the Internet, or some more particular form of networked communication.

Drawing a comprehensive list of third parties which may be involved in the processing of Internet communication can be a quite daunting and lengthy exercise. However, a basic and succinct division in representative categories includes:
(a) Network operators, mobile telecommunications providers, and access providers (generally known also as "Internet Service Providers" or "ISPs" in the narrow sense);
(b) Website hosting companies, including portals, dedicated server space and domain name registrars;
(c) Information location tools and content aggregators;
(d) E-commerce platforms and online marketplaces;
(e) Providers of online services, such as e-mail and cloud computing, which allow user-to-user communications or host user-generated content;
(f) Network-related hardware manufacturers, such as computer and mobile manufacturers
(g) Network-related software and applications developers, such as companies designing anti-virus programs and filtering technologies.

Other entities, which are not necessarily an intermediary from a technical perspective but whose activity is *de facto* instrumental to enable users to receive and impart information, include payment systems, advertising networks, cybercafés, and even the users themselves (for instance, when they "tweet" or otherwise (re)transmit manifestly illegal content). Legitimate questions arise as to whether the activities of these entities should be dealt with under the same rules and standards as more traditional types of intermediation. In the absence of an explicit recognition of uniformity, courts and legislators around the world are either struggling to find a proper qualification, or exploiting the vacuum to impose heightened standards of liability[11]. More research work is therefore needed to

[10] See "intermediary" in Oxford Dictionaries, available at http://oxforddictionaries.com/definition/english/intermediary

[11] Mark MacCarthy, "What Payment Intermediaries Are Doing About Online Liability and Why It Matters" Berkeley Technology Law Journal (2010) 1037; Organization for Economic Cooperation and Development *The Economic and Social Role of Internet Intermediaries*, DSTI/ICCP/ICCP(2009)9/FINAL (Apr. 2010), p.13; European Commission, "EU Commission presents plan to better protect and enforce intellectual property law" (Press Release, July 1st, 2014), available at http://europa.eu/rapid/press-release_IP-14-

properly define the reach and form of intermediary liability regimes in these increasingly important areas. For the sake of clarity and simplicity, the following section refers to the categories identified by the legislators in US and EU, which determine the modality and scope of protection of the different types of intermediation in the respective jurisdiction.

3. Distinguishing types of intermediation: the American and the European approach

Historically, the first and leading reference for the identification of different types of intermediaries has been the US Digital Millennium Copyright Act, and in particular its Section 512, which provides detailed rules for the limitation of intermediary liability in the copyright context. For the present purposes, it is useful to make an overview of the intermediaries described in that section, so as to provide a benchmark for comparison with other relevant normative frameworks. As it can be seen from a glance through the main provision of this Section as well as other international references[12], safe harbors generally cover three types of intermediation: (1) communication conduits; (2) content hosts; and (3) search service and application service providers.

(1) Communication conduits. Section 512 (a) covers the most passive category of ISPs, those offering "Transitory Digital Network Communications", comprising any activity of "*transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections*". In light of the necessary and unavoidable character of these activities for the unfolding of Internet communications, this section confers an immunity from civil liability for user-generated content, provided that such activity is (a) initiated by the user and directed to the designated recipient(s), and (b) it is done through automated process without (c) any modification or selection of the content or (d) of the recipient, and (e) with no copy of the material made available in a manner ordinarily accessible to anyone other than anticipated recipients, or maintained for longer than necessary. In light of its crucial importance for the unfolding of network communication, this exemption repeats itself under the same conditions (although different wording) in virtually all intermediary liability regimes.
Section 512 (b) addresses another type of conduit activity –system caching- which consists of "*intermediate and temporary storage of material on a system or network*" undertaken for the purpose of enabling subsequent users to access material made available by one particular user (the "cacher"), generally to overcome network connectivity issues and guarantee a ready and speedy access to content. This section, which applies not only to "ISPs" in a narrow sense, but more generally to any provider of

760_en.htm ; Nandan Kamath, "Should the Law Beat a Retweet? Rationalising Liability Standards for Sharing of Digital Content" Indian Journal of Law and Technology 9 (2013); Gbenga Sesan, "Intermediary Liability in Nigeria", Association for Progressive Communications Intermediary Liability Research Papers N. 3; available at https://www.apc.org/en/system/files/Intermediary_Liability_in_Nigeria.pdf; Center for Internet and Society India, "Comments on the Information Technology (Guidelines for Cyber Cafe) Rules, 2011"; available at http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011

[12] OECD, *The Economic and Social Role of Internet Intermediaries*, DSTI/ICCP/ICCP(2009)9/FINAL (Apr. 2010)

services on the Internet (hereinafter, "ISPs")[13]. This section, too, defines a safe harbor and requires for that purpose that the content be not modified, as well as that the service provider comply with rules concerning the refreshing, reloading, or other updating of the material or any other conditions specified by the person making the material available online in the first place [14]. Moreover, upon notification of a claim of copyright infringement over the cached material, the service provider must expeditiously remove or disable access to the material claimed to be infringing, provided that the notification includes the acknowledgement that the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered so. It should be noted that caching is not specifically addressed by all intermediary liability regimes, and they are often covered by a more generic formulation of the "conduit" exemption (for instance, in Canada[15]) or by a broad exemption for intermediaries based on knowledge of illegality (for instance, in China[16], Japan[17] and South Korea[18]).

(2) Content hosts. Section 512 © is devoted to a different type of storage ("Information Residing on Systems or Networks At Direction of Users",") which occurs "*at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider*": for example, this would include cloud computing services or simple email storage. The provider of these services benefits of a safe harbor only if it fulfills three sets of conditions: (1) does not have actual knowledge of the infringing nature of the material, and is not aware of facts or circumstances from which infringing activity is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and upon notification of claimed infringement, responds expeditiously to remove, or disable access. (3) has a designated agent for the notification of claims of infringements and follows the special procedure of notice and take-down indicated by Section 512 (g).

(3) Search service and application service providers. The following section, 512 (d), is concerned with immunity for the provision of information location tools, "*including a directory, index, reference, pointer, or hypertext link*". These services differ from hosting in that they facilitate access to content, but do not necessarily host it. The conditions to be

[13] For instance, a District Court in Nevada found certain practices of Google's search engine to constitute "caching" for purposes of section 512 (b): see *Field* v. Google, *Inc.*, 412 F. Supp 2d. 1106 (D. Nev. 2006)

[14] The conditions that the "cacher" can specify include the technology to be used, except to the extent that it significantly affects the performance of the network and it is not in line with industry standards communication protocols

[15] See Copyright Act of Canada, chapter 42, section 2.4. (1) (b)

[16] Ordinance of the Protection of the Right to Network Dissemination of Information , [promulgated by the State Council, May 18 , 2006, effective July 1, 2006], art 21, LAWINFOCHINA (), *translated in* Intell. Prop. Prot. in China, http://english.ipr.gov.cn/ laws/laws/others/235897.shtml

[17] See Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Effective November 30, 2001), Unofficial translation, available at http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/H13HO137.pdf

[18] See Korean Copyright Act, ch. 6 (1986), translated in http://eng.copyright. or.kr/law_01_01.html

fulfilled by service providers to benefit of this safe harbor are identical to those imposed by section 512 ©.

The last category of intermediaries is described by section 512 (e) as " Nonprofit Educational Institutions" who are acting as service providers for their staff, such as faculty members and graduate students performing teaching or research. This section clarifies that such individuals' infringing action, as well as their knowledge or awareness of the infringing nature of their activities, shall not be attributed to the institutions concerned[19] -at least as long as the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, US copyright law. This category is often left out of the commentaries on US intermediary liability as its focus is on the finality of the intermediated communication, rather than on the distinctiveness of a particular technical activity performed through the use of the network. Although this provision appears largely redundant because the exemption from liability of the technical service described therein can be accommodated through the other safe harbors[20], it should be acknowledged that its inclusion into the safe harbors gives educational institutions greater certainty, and may be a useful reference in thinking about the activities covered by a definition of intermediaries outside the copyright realm. .

The categories identified by the DMCA are rather narrow, which is in part a consequence of the fact that they were drafted with a view to providing limitations exclusively to *copyright* liability. Other types of liability, including in other areas of IP, are dealt with by a general norm (47 U.S.C. 230, introduced with the "Communication Decency Act" or "CDA"), which gives complete immunity for good faith editorial choices to any provider and user of an interactive computer service for information created or developed by another person or entity. Unlike the DMCA, this provision adopts a broad understanding of intermediary, defining "interactive computer service" as "*any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions*[21]" and ultimately considering intermediary not only the provider, but any user of such service who exercises technical or editorial control over the content created or developed by others.

Finally, the picture on online intermediary liability in the US would be incomplete without mentioning section 32 (2) Lanham Act, which shields publishers of a periodical

[19] Except for those special situations where the infringing material had been used or recommended for a course at the institution in the previous 3 years, and the institution had received more than two good faith notifications of copyright infringement by that staff member.

[20] By contrast, online activities provided by public educational institutions are explicitly excluded from the scope of the EU E-commerce Directive, since this is applicable only in relation to information society service providers and information society service required to be "normally provided for remuneration".

[21] See Section 230 (f) (2) and (3). Furthermore, section 230 (f) (4) clarifies that "access software provider" refers to a provider of software or enabling tools that do any one or more of the following:
(A) filter, screen, allow, or disallow content;
(B) pick, choose, analyze, or digest content; or
(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content".

or electronic communication that are "innocent infringers and innocent violators" (a notion that is still subject of controversy) from damages and certain injunctions for contributory trademark infringement[22]. This safe harbor also limits the possibility for a claimant to obtain injunctive relief in circumstances where an injunction would interfere with the normal operation of the online publisher[23].

The resulting patchwork arrangement has been criticized for lack of consistency, due to the possibility for plaintiffs to characterize the same pattern of facts as either a general tort claim, or a more specific copyright or trademark claim: in practice, this can lead to litigation abuses, as well as to intermediaries refraining from exercising editorial discretion in doubtful situations, so as not to risk falling outside the copyright safe harbor[24]. He therefore suggests to "standardize" safe harbors so as to provide consistency across different areas of law. For an horizontal (across-domain) approach to intermediary liability, one needs to look no further than the adoption of the European Copyright Directive 2000/31 (ECD) to find a term of comparison.

Similar to section 512 but not limited to the field of copyright, the European E-Commerce Directive 2000/31 (ECD) devotes four articles (12-15) to the regime of liability of "information society service providers", whereby an "information society service" is defined as "*any service normally provided for remuneration*[25]*, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service*[26]". This definition is broad enough to encompass a variety of services, including mere access providers, but features a couple of important differences from the DMCA model: first, it requires in all such cases (and not only) that the service is provided at the individual request of the recipient, thereby ruling out radio and TV broadcasting. Second, it rules out those services that cannot be provided entirely at distance. It should be added that Recital 18 of the ECD clarifies that the notion of "remuneration" does not mean that services shall necessarily be given in exchange for a fee, so long as they can be qualified as part of an "economic activity".[27]

---

[22] See 15 USC , Section 1114(2)(B)

[23] See 15 USC , Section 1114(2)(C)

[24] Mark Lemley, Rationalizing Safe Harbors, *Journal of Telecommunications and High Technology Law*, Vol. 6, p. 101, 2007, 109

[25] Recital 19 clarifies that this is not the case, for example, for public education and governmental services.

[26] See art. 2 (a) of the Directive, referring to the definition in art. 1(2) of Directive 98/34, as amended by Directive 98/48

[27] According to Recital 18:

"Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; *information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them*, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at

(1) Communication conduits. Article 12 of the directive refers mainly to IAPs and other providers of technical services, identifying the activity of "mere conduit", as "*the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*". Like the DMCA, the Article requires that the ISP does not select or modify the content or the receiver of the transmission, and that no storage is made other than for the sole purpose of carrying out the transmission in the communication network, and for no longer than is reasonably necessary for the transmission. The problems with this article have been identified by a EU study as the lack of definition of "communication network" and the uncertainty over whether filters would be considered to select or modify the content[28].

Article 13 deals with caching, defining it in a much similar way to in the DMCA as "*the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request*", and requiring for purposes of the safe harbor that the provider does not modify the content, complies with the rules regarding the updating of the information and the conditions on access to the information, and (an obligation that is less explicit in the text of the DMCA) does not interfere with the lawful use of technology to obtain data on the use of the information. Moreover, the provider must operate consistently with the rule that, in case of notification of the removal of the "cached" material from the network or the disabling of access to it or the ordering by a court or (unlike in the DMCA) an administrative authority in this sense, it must act expeditiously to do so. With respect to the activities identifed by this definition, the EU study noted that it is not entirely clear whether it would encompass decentralised content distribution systems such as Usenet groups and peer to peer networks[29].

(2) Hosts. Article 14 addresses "hosting", defined as "*the storage of information provided at the request of a recipient of the service*", and confers immunity provided that: (a) the provider does not have actual knowledge of illegal (either civil or criminal) activity or information, nor (as regard claims for damages) has awareness of facts and circumstances from which such illegality is apparent. (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information; and (c) has no authority or control over the recipient.

This is without doubt the most controversial safe harbor of the ECD, for several reasons. First, it does not specify what counts as "actual knowledge", therefore allowing EU

---

individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; *activities which by their very nature cannot be carried out at a distance and by electronic means*, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient *are not information society services*" (emphasis added).

[28] EU Commission, Chapter 6, *EU study on the Legal analysis of a Single Market for the Information Society. New rules for a new age?* (2009), p.14

[29] Ibid., 15

member states to adopt different approaches in the implementation of the Directive, such as requiring a formal notification by the competent administrative authorities (as in Spain), the fulfillment of a notice and take-down procedure (as it's the case in Finland), or leaving the determination to national courts on a case by case basis (like in Germany and Austria). Aside from that, this safe harbor does not require the following of a notice and take-down procedure for the processing of notifications, thereby leaving intermediaries with the uncertainty of several potentially conflicting legislations, not only within the EU but also worldwide. Third, it is not clear the extent to which the activities of the intermediary should consist of hosting, as the European courts' interpretation has ranged from "some" to "the majority", "the most important part", and more recently, the European Court of Justice has shifted the focus onto whether the service was neutral with respect to the content hosted or there had been an adoption[30].

Further inconsistency is generated by the fact that there is no specific provision covering the conduct of providers of information location tools, which in the DMCA are dealt with separately. This has caused EU member States to adopt diverging approaches to their liability, with Austria for example extending the protections of "mere conduits" ex art. 12 of the Directive, and Spain, Portugal and Hungary explicitly extending the protections of art. 14 (but in the case of Hungary, not to hyperlinks)[31]. Besides these macro divergences, several smaller but important variations exist on issues such as the extent to which injunctions are available against intermediaries[32], and the conditions for the disclosure of the identity of alleged infringers[33].

In conclusion, while a certain degree of inconsistency exists in the US between the standards adopted for intermediary liability in different areas of law, in the EU an inconsistency both within and across jurisdiction stems from the imperfect harmonization effort undertaken by the EUCD, despite the clear intention of the EU to create with it a uniform horizontal treatment of the responsibility of intermediaries.

4. "Disruptive innovation" at work: the Brazilian approach

The situation in Brazil regarding intermediary liability was until 2014 one of complete absence of specific rules; this led courts to treat it on the basis of general principles of

[30] *Ibid.*, 16

[31] The case of liability for linking is a particularly controversial one across EU member states: for example, the UK Cyprus introduced a regulation which obliges host providers to stop providing hyperlinks to illicit contents (section 17 (1) lit. c Act N° 156(I)/2004 of 30/04/2004). In UK, a court considered "deep linking" (i.e., linking directly to the content page without passing through the content provider's home page) to constitute copyright infringement for inducing to skip the provider's advertisements. See *Court of Session: Outer House 24.10.1996 -1997 F.S.R. Shetland Times, Ltd. v. Dr. Jonathan Wills and Zetnews, Ltd. By* contrast, in a landmark case the German Federal Court of Justice held that deep links were described as being socially desirable information location tools, precisely as the database operator is able to protect himself by diverting all links directing to the specific web-site to the root site, i.e. to the main portal, so that his interest in earning advertising income can be satisfied by technical means.

[32] See Nicolo Zingales, "Internet Intermediary Liability: Identifying best practices for Africa" (Association for Progressive Communication, August 2013).

[33] See Nicolo Zingales, "Virtues and perils of anonymity: Should intermediaries bear the burden?", Journal of Intellectual Property, Information Technology and E-Commerce Law, 5(3), 155-17

civil and consumer protection law, under a very high standard of care[34] sometimes comparable to strict liability[35]. It also led to a series of private agreement between copyright holders, ISPs and other internet services[36] and to the affirmation of a set of informal norms around notice and takedown that has proved "very compliant with industry demands"[37].

Despite the effectiveness of this system for prompt removal of copyright infringing material, copyright owners were still uneasy about the possibility for users to play "whack a mole" with copyrighted content, uploading it swiftly and with impunity shortly after removal. In other words, absence of a procedure for obliging ISPs to hand over or even retain subscriber data manifested itself as a key challenge to the effectiveness of copyright protection *vis a vis* repeated infringers. For this reason, a bill (the Azeredo Bill) was introduced in 2008 imposing a 3-year mandatory period of data retention, and requiring ISPs to collaborate in the disclosure of the identity of infringers. The Azeredo Bill also criminalized the access to data "without authorization of the legitimate owner", foreseeing a sanction of 2 to 4 years of jail, thereby turning into felony overnight the conduct of approximately 60% Brazilians[38]. Inspired by the CoE Convention on Cybercrime, the bill was attempting to enact a criminal statute without even having in place a civil framework for the Internet- which was the case for the great majority of the States parties to the Convention[39].

This is the background from which the Marco Civil do Internet (Federal Law No. 12965/2014, previously Bill No. 2126/2011), gradually came into being: civil society, firmly rejecting the measures put forward in the Azeredo Bill, launched a campaign of fierce opposition (which became known as "Mega Não) and generated consensus over the need to develop a civil framework in respect of the civil rights and liberties of Brazilian citizens. This led to a partnership between the federal government and the Center for Technology and Society of the Law School at the Fundação Getúlio Vargas (CTS/FGV), resulting in proposals and the creation of an innovative platform for online public consultation, which allowed everyone to comment and contribute to the drafting of the bill.

---

[34] See among others, Superior Court of Justice, Fourth Panel, *Google Brazil*, Special Appeal no. 1306157/SP, March 24, 2014

[35] See Ronaldo Lemos, Carlos Affonso Pereira de Souza, Sergio Vieira Branco Jr., Pedro Nicoletti Mizukami, Luiz F. Moncau, and Bruno Magrani. 2009. Proposta de Alteração ao PLC 84/99 ; PLC 89/03 (Crimes Digitais). Rio De Janeiro: Center for Technology and Society, Getulio Vargas Foundation (http.virtualbib.fgv.br/dspace/bitstream/handle/10438/2685/Proposta_e_ Estudo__FGV-CTS_Cibercrimes?final.pdf?sequence=1

[36] See Pedro Nicoletti Mizukami, Oana Castro, Luiz Fernando Moncau, and Ronaldo Lemos, "Chapter 5: Brazil", in Joe Karagnis (ed.), *Media Piracy in Emerging Economies*; citing data from the International Intellectual Property Alliance), particularly the special 301 Report on Copyright Protection and Enforcement (2009, Washington, DC: IIPA).

[37] Ibid.

[38] Osvaldo Saldias, "Coded for Export! The Contextual Dimension of the Brazilian Marco Civil da Internet", Alexander von Humboldt Institute for Internet & Society Discussion Paper 2014-06

[39] Ronaldo Lemos, Internet brasileira precisa de marco regulatorio civil. UOL Tecnología, 22 May 2007, available at http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm

Between 2009 and 2010 the public consultation gathered approximately 2,000 comments (respectively, 800 and 1180 in each of its two phases); in addition to that, contributions were collected via other channels, including by scanning social media for dedicated commentary and receiving direct submissions. In 2011, the bill was signed by the executive and sent to Parliament, where Alessandro Molon was appointed as its rapporteur. Having organized a series of events and a further consultation for the proposed text, Molon cleared the bill for voting on July 2012; however, the approval was repeatedly delayed (until March 2014) due to strong pressures on particular provisions, including: (1) on intermediary liability, the clash between telecommunications companies and Rede Globo, a powerful media group representing a significant player in the copyright industry in Brazil; (2) on data retention, the clash between civil society, federal police and other sectors engaged in the fight against cybercrime; and finally (3) on network neutrality, the clash between telecommunication providers and content providers[40].

The Marco Civil is also known as "Constitution of Internet" because it creates the rules of engagement on the network, and does that based on the affirmation of a number of pillars to safeguard civil liberties, such as the privacy and freedom of expression of users. In fact, freedom of expression is explicitly erected as the main pillar for the discipline of Internet use in Brazil (art. 2), as well as (i) the recognition of the global scale of the network; (II) human rights, personality development and the exercise of citizenship in digital medias; (III) plurality and diversity; (IV) openness and cooperation; (V) free enterprising, free competition and consumer protection; and (VI) the social purpose of the network. Likewise, the Marco Civil explicitly recognizes (art. 3), among other things, the guarantees of freedom of expression, privacy and liability of the agents according to their activities (i.e., not for activity of others) pursuant to the law, as well as security, stability and neutrality of the network; this along side the recognition of the freedom of business models promoted on the Internet, provided they do not conflict with the aforementioned principles. Finally, the law is founded (art. 4) on the aims to promote (I) the right of all to access the internet; (II) the access to information, knowledge and participation in the cultural life and in the handling of public affairs; (III) the innovation and the stimulus to the broad diffusion of new technologies and models of use and access; and (IV) the adoption of open technology standards that allows communication, accessibility and interoperability between applications and databases.

As an implementation of those principles article 8 establishes, after reaffirming the right right to privacy and freedom of expression in communications as a prerequisite for the full exercise of the right to access the internet, that any contractual clause in breach of the above mentioned provisions (including those affecting the inviolability and secrecy of communication[41]) will be considered null and void.

[40] See Veridiana Altomonte, "Marco Civil: a civilian reaction to surveillance on the Internet", GSI Watch 2014 (2014), available at http://www.giswatch.org/en/country-report/communications-surveillance/brazil

[41] In that regard, article 10 provides that the content of communications may only be made available by court order, and any operation of collection, storage, retention and treating of personal data or communication data taking place (at any point in the chain of these acts) in Brazil must comply with Brazilian law.

While the battle over net neutrality was settled with the need to define the appropriate regulation at a later (upcoming) stage, the fight over data retention resulted in a steep decrease of the mandatory period of 3 year proposed in Azeredo Bill, equal to 1 year for the storing of connection data and 6 months for the records of access to internet applications (so called "logs"). By contrast, the solution to the controversy regarding intermediary liability strikes as much more complex and articulated. First, a very important principle is laid out in article 18, which establishes that the provider of connection to the internet shall not be liable for civil damages resulting from content generated by third parties: this is a strong version of the "mere conduit" principle contained in the EU and US legislation, without any exceptions concerning the initiation or modification of the transmission, nor any mention of the technological means used to accomplish transmission. Secondly, article 19 limits the possibility of liability for internet application providers (broadly analogous to "content hosts") to cases where they fail to remove illegal content upon specific judicial order. It also enables judges to issue injunctions anticipating the effects of the request, upon fulfillment of the requisites of likelihood of success and irreparable damage (or damage that is difficult to repair). Third, article 21 establishes a special provision for breach of privacy arising from the disclosure of images, videos and other materials containing nudity or sexual activities of private nature, without the authorization of participants: this is known as the "revenge porn" exception (despite the fact that neither the pornographic character nor the intention of revenge constitute a requirement), and it imposes liability of internet application providers for failure of due diligence if they have failed to remove once they have received a request of removal by the interested party or his/her legal representative. Finally, the Marco Civil in closing (art. 31) makes an specific exemption for the liability of internet application providers, in case of copyright or related rights: the applicable procedure in force will remain that of the existing copyright law, up and until the entering into force of a specific copyright regulation, which is currently under discussion at the Parliament (since 2010). It is clear that, in particular as a result of the intense pressure from the copyright industry, this was too sensitive of an issue to be dealt with under the framework of the Marco Civil; accordingly, this exception was crafted to prevent the blocking of the bill by the cultural production industry, spearheaded by Globo[42].

All in all, it is apparent that the Marco Civil was the result of significant compromise between different constituencies. Nevertheless, the opening to multistakeholder participation at all stages of the bill did not prevent it from achieving quite far-reaching positions of guarantee for individual rights, particularly on privacy and freedom of expression. In this context, the enunciation of two important principles of intermediary liability (that such liability is excluded for conduits, regardless of the means of operation; and that the same applies to content hosts, as long as they have not received a judicial order to remove content) is a remarkable achievement which reinforces the guarantees enshrined in this document, and should be seen as an inspiration for legislators around the globe.

5. Embracing heterogeneity for the way forward: a taxonomy of the existing options

[42] See Mariana Giorgetti Valente and Pedro Nicoletti Mizukami, "Copyright Week: What Happened to the Brazilian Copyright Reform?", Info Justice (Jan 20, 2014)

In order for the appropriate regime to be framed, legislators need to account for the different sets of incentives and potential harm that are generated in different areas of law, as well as with regard to the peculiarities of different kinds of intermediation. This can be done by confronting pros and cons of different models of intermediary liability for user-generated content. Seven main alternatives can be identified:

(A) Full immunity, such as the one conferred by the US Community Decency Act (section 230). This option is the least intrusive into the free flow of information, but by leaving the judgment entirely to private entities, it carries the risk of arbitrariness and lack of due process in the determinations of what is to be removed.

(B) Immunity upon respect of the notice and take-down procedure, such as the one provided by US Digital Millennium Copyright Act (section 512). While this model allows greater user interaction, with responsibility for lack of removal triggered only upon notice not followed by an adequate response by the content provider, it carries the risk of abuse to the extent that it does not require due diligence of the claimant before sending the notification. Therefore, it exposes the content provider to potentially unjustified claims: as such, the model is more conducive to removals of content than to free speech. It might be more balanced with the insertion of specific exceptions, such as the fair use defense, and an obligation for ISPs to put back material which is plausibly defended as legal after removal.

(C) Responsibility upon failure to act combined with actual or constructive knowledge of illegality of the user's content, such as the one imposed by the EU Copyright Directive. The main problem with this model is the vagueness of the notion of constructive knowledge, which has been interpreted by courts in different manners, and likewise the lack of harmonization with regard to the user's participation in the final determination of the authority. Thus, a clearer provision is desirable, if this model is to be retained at all. One area which would appear to be well suited for the application of this concept is that of cybersecurity, where it is objectively easier to identify the standards of "due diligence" in the field.

(D) Responsibility upon failure to execute the order of an administrative authority - as it is the case under France's "Hadopi Law"[43]. This model, which is currently adopted through self-regulation of Internet service providers in South Africa [44]and entered into Italian law as part of the copyright reform in Italy in 2014[45], can be deployed only to the extent that it incorporates safeguards for the respect of the user's right to be heard: in 2009, the French Constitutional Court held the first version of the Hadopi law unconstitutional precisely because it did not afford sufficient due process rights and because the presumption of innocence was infringed by giving presumptive force to the determination of a non-judicial

[43] République française (2009) Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, Journal Officiel de la République Française, 13 June, 135: 9666.

[44] See "World Intermediary Liability Map: South Africa"; available at http://cyberlaw.stanford.edu/page/wilmap-south-africa

[45] See "World Intermediary Liability Map: Italy"; available at http://cyberlaw.stanford.edu/page/wilmap-italy

authority[46]. Arguably, this model is more appropriate in proceedings where considerations of public order and morality are at stake, such as with obscene content.

(E) Responsibility upon failure to execute the order of a judicial authority- as it is the case under Brazil' s general clause in the Marco Civil. This model ensures the balancing of different rights and interests before a court of law, and thus it is appropriate for disputes of particularly complex nature. However, applying this model to all disputes might lead to private agreement as an alternative to circumvent the slowness of the process, as it occurred in Chile for example[47].

(F) Responsibility upon failure to grant a request from the interested party or his/her representative – as it is the case under Brazil's "revenge porn" exception in the Marco Civil. This model is more appropriate for the deletion of materials affecting the virtual identity of individuals beyond cases of obscenity, reaching into scenarios of intimacy and potentially being valid also for legitimate "right to be forgotten" requests.

(G) Responsibility upon failure to remove previously detected illegal material: this is the case of pedopornographic material, where the engagement of intermediaries tend to be scrutinized very strictly[48]. Unless the identification of such material occurs otherwise, this can be normally subsumed under (D), although a stricter standard might apply here in comparison with other types of administrative procedures.

What the above list makes clear is that there is no unique solution for all types of problems involving intermediaries. However, due to the lack of a global forum for standard-setting in these different areas, we live the unsettling situation in which legislations around the world pick one model or another without sufficient reflection of the implications of a broad formulation of this regime. As a matter fact, uncalibrated intermediary liability regimes can have an impact on the effectiveness of the operation of other regimes, including not only those established in different cognate areas but also those in place in different countries, a clash against which may become a routinary challenge in our global interconnected society. For this reason, it is submitted that the creation of a forum for the definition of intermediary liability regimes would constitute an important advancement for Internet governance in the years ahead. This would prevent not only friction between regimes, but also the overriding of existing solutions by means of private agreements conceived to addressed the unsatisfactory treatment of some

[46] Under the original version of the law, the user could escape liability by rebutting the presumption of guilt associated with his address, by proving that he or she was subject to fraud perpetrated by a third party. However, the French Constitutional Court invalidated several provision of this law on the basis of the recognition that, while as an exceptional measure a presumption of guilt may be introduced, particularly in the case of minor offences, this is only acceptable if such presumptions are not irrebuttable, if the rights of the defence are respected and if the available facts tend to confirm the likelihood of the commission of the incriminated act. See French Constitutional Council's decision No. 2009-580DC of 10 June 2009 (at 17-18), available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf

[47] See "World Intermediary Liability Map: Chile"; available at http://cyberlaw.stanford.edu/page/wilmap-chile

[48] See e.g., in Brazil, Lei 10.764/03 sobre o Estatuto da Criança e do Adolescente e dá outras providências.

of the particular interests at stake. What past experience has shown is that, in the absence of a copyright-specific regulatory solution, representatives of the intellectual property constituency tend to prevail over other stakeholders and skew the balance of the whole process -arguably due to their superior expertise, coordination and rhetoric- at the expense of a more disperse and less resourceful representation of users and civil society.

This happened not only in the example made *supra* (section 1) about the UK, but also in the latest attempt to establish global provisions on intermediary liability within a charter of "Principles" of Internet governance: the Global Multistakeholder Meeting on Internet Governance (NETmundial). While the original text which resulted from a call for online contributions had no specific provision on intermediary liability, the new text which was drafted on the basis of the inputs received at the NETmundial meeting included the principle that "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". As noted elsewhere[49], this formulation is problematic to the eye of civil society because the focus on economic aspects prevails over the protection of human rights- precisely the opposite of what Marco Civil suggests. Those who were present at the meeting witnessed that this compromise was the result of intense lobbying from the copyright industry[50]; in other words, the whole model for intermediary liability in internet governance seems to be calibrated on the basis of the needs of copyright (and perhaps trademark) owners.

Given these circumstances then, it is not surprising that the drafters of the Marco Civil decided to exempt copyright from the application of the established intermediary liability regime, remanding to a specific regulation that is currently under discussion with the copyright reform bill. Nevertheless, the Marco Civil demonstrated the feasibility of a multistakeholder consensus on principles, mostly of procedural nature, which are crucial for intermediary liability. In doing so, it may have provided a blueprint for the creation of a global Internet Constitution- some would call it "Magna Carta" [51] - to frame intermediary liability regimes around the respect for fundamental rights. The establishment of such principles at the international level would have tremendous

[49] See Marilia Maciel, Nicolo Zingales and Daniel Fink, "The global multistakeholder meeting on the future of internet governance (NETmundial)". *Multistakeholder as governance groups: Observations from case studies* (Berkman Center Research Publication 2015-001), pp. 214-237, noting that the second sentence of the text contains a provision which recalls the controversial OECD's language of voluntary measures to deter infringement in accordance with "fair process"- as opposed to the more stringent right to 'due process' which forms integral part of human rights jurisprudence. Cf. Communique' on Principles for Internet Policy-Making, at http://www.oecd.org/internet/innovation/48289796.pdf. , which civil society did not endorse precisely in light of the vague terminology and the risk that this would lead to censorship: for an account, see Milton Mueller, "Civil Society Defects from OECD Internet policy principles", Interne Governance Project blog, http://www.internetgovernance.org/2011/06/28/civil-society-defects-from-oecd-internet-policy-principles/

[50] Gabrielle Guillemin, "Netmundial: success or failure?", Article 19's blog (April 29th, 2014), available at http://www.article19.org/join-the-debate.php/143/view/

[51] See Jenima Kiss, "An online Magna Carta: Berners-Lee calls for bill of rights for web", The Guardian (March 12th, 2014); available at http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

implications on the advancement of a common understanding of the role of intermediaries in our interconnected society, and would avoid a great deal of friction generated by the different standards that are continuously being devised, adjusted and modified.

6. Setting the pillars for a human-rights compliant model for intermediary liability

In order to achieve a balanced framework for the regulation of intermediary liability, it is wise to proceed on the basis of a number of pillars, which, much like in the Marco Civil, can serve as guidance for the drafting of more specific provisions, including those concerning the conduct expected from intermediaries.

Modeling an "ideal" regime requires an acceptance of the essential rule of law requirements which are at the basis of our understanding of the Internet as an enabler of development, communication and innovation. The following constitute the five principles which most clearly enshrine these ideals, and which can thus be fruitfully erected as pillars for the future cooperation on global intermediary liability discussions.

(1) Freedom of expression. At its core, the development of and through the Internet are founded on the ability to connect people and let information flow among them, which is conceptually anchored on idea of openness and global, unrestricted access to information and ideas. A very useful departure point in this respect is the 2011 Joint Declaration of the three Special Rapporteurs for Freedom of Expression, which contains a specific section on intermediary liability. The declaration restates the "mere conduit principle" (as enunciated in virtually every regime of intermediary liability) and suggests considering the possibility of limiting the liability of other intermediaries under the same conditions. Additionally, the Rapporteurs warn against the imposition of duties to monitor and against extrajudicial content takedown rules which (as it's the case under several regimes) fail to provide sufficient protection for freedom of expression. This is complemented by an encouragement to adopt self-regulatory solutions for the management of rights online, which must be read in conjunction with the importance of safeguards for individual liberties, a system for intermediary liability must lay out with clarity. Such safeguards would imply for example, the need for stringent conditions for the disclosure of the identity of suspected infringers – which is precisely what the copyright industry is managing to accomplish (via private agreements) in the absence of a dedicated forum of dedicated discussion of the topic.

(2) access. Without equal and effective access to the Internet, the ability of "netizens" to receive and impart ideas is undermined in the first place, thereby compromising the series of benefits that such "flow of information" can bring about. In this sense, it can be considered that access is a requisite that must pre-exist for the development of Internet freedom. As to the essential characteristics that a full embracement of the concept of access requires, "equality" recognizes the importance of creating a level playing field where all individuals have the same opportunity to engage in communication, and "effectiveness" refers to the existence of a minimum standard of quality of service that ensures that such opportunity is not being impaired in practice by the operation of technical or legal obstacles.

(3) privacy. This is a concept that is intrinsically connected to the idea of free expression, in at least two different ways: first, the respect for privacy serves as a limitation to the scope of the right to freely express oneself. Second, the possibility to control the information that we make available to the public enables us to engage in communication more freely.

(4) due process. This is a notion that is also used in a variety of contexts, and which can therefore give rise to confusion. It represents the foundation of a democratic society on the rule of law, as opposed to rule by law[52], which in the words of the legal scholar who is considered to have founded this concept, is grounded on the notions of equality before the law, absolute supremacy of the law over arbitrary power; and interpretation and enforcement of the law by the courts[53]. Putting this concept into more concrete terms, due process refers to those procedural rights which a state "owes" to members of the legal system that are subject to specific individual determinations, specifically imposing the existence of the following minimum requirements to enable any affected party to present their case: (a) a form of legal process which respects the guarantees of independence and impartiality; (b) the right to receive notice of the allegations and the basic evidence in support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (c) the right to a reasoned decision, addressing every essential claim in the matter under dispute[54].

(5) Free and open Internet. This is a principle from which emanate important consequences for the free flow of information and ideas, although not necessarily accruing immediate rights to individuals. In line with this principle, a developmental perspective has defined Internet freedom around the concepts of "openness" and "permissionless innovation"[55], both alluding to a collaborative environment where users are significantly free to develop new ideas without being "held up" by proprietary technologies or rigid legal or technical mechanisms.

In accordance with the above principles, a very useful departure point in the search for a global regime is the 2011 Joint Declaration of the three Special Rapporteurs for Freedom of Expression, which contains a specific section on intermediary liability. The declaration restates the traditional "mere conduit principle" (applicable in virtually every regime of intermediary liability) and suggests considering the possibility of limiting the liability of other intermediaries under the same conditions: in other words, treating intermediaries uniformly by exempting them from liability to the extent that they do not initiate the transmission or select its receiver, or modify the information contained in the transmission. This enables automatic services provided upon request to develop without

[52] Tom Ginsburg and Tamir Moustafa, *Rule by law: the politics of courts in authoritarian regimes* (Cambridge University Press, 2008)
[53] Albert V. Dicey, *An introduction to the Study of the Law of the Constitution* (10th ed., 1959), pp. 202-203
[54] See Nicolo Zingales, *Right to be Heard and Presumptive Reasoning in Public Economic Adjudication: The Case of EU Antitrust Enforcement*, Doctoral Thesis submitted at Bocconi University (May 2013)
[55] Global Voices Online, "Internet Declaration", 4 July 2012, http://www.internetdeclaration.org/freedom; Barbara Van Schewick, *Internet Architecture and Innovation*" (MIT Press, 2012)

the threat of potential litigation, simultaneously enabling speech and maintaining the incentives for the creation of innovative business models.

The other side of the coin, however, is that immunity may also generate perverse incentives on some of the rights at stake, such as privacy, due process, and even the very same freedom of speech that the qualified immunity is meant to serve. Often, the harmful speech of one implicates the end of the free speech of another. The problem lies precisely at the juncture of these interests: who defines what is "harmful"? As long as the definition in this level of detail will not be comprehensively dealt with by an overarching framework, intermediaries will continue to be the *de facto* regulators with *carte blanche* in the determination of what conduct or content is allowed within their services.

On this aspect, the Rapporteurs' message seems to hold back in order to leave space for creative solutions in the definition of intermediary liability regime; however, at the same time it calls against the imposition of duties to monitor the [legality of] the activity taking place within the intermediaries' services, and against the adoption of extrajudicial content takedown rules which (as is the case under several regimes) fail to provide sufficient protection for freedom of expression.

What we are left with, then, is significant freedom for intermediaries to adopt self-regulatory solutions for the management of rights online, which the Rapporteurs indeed encourage. However, this should be read in conjunction with the recognition of the importance of minimum safeguards for individual liberties, which in accordance with the Declaration and other international human rights document, must be laid out with clarity by the law. Such safeguards would imply, for example, the need for stringent conditions for disclosure of the identity of suspected infringers – which is precisely what is lacking in the agreements that the copyright industry is currently stipulating in various countries in the absence of a dedicated forum of discussion on the topic. Not only privacy, but also freedom of expression, due process, access and free and open Internet should be institutionally embedded into intermediary liability regimes of any form and dimension.

Conclusion

…