Internet intermediary liability: Identifying best practices for Africa

by Nicolo Zingales*

Association for Progressive Communications (APC)

Independent research commissioned by the Association for Progressive Communications and supported by Google Africa

*I thank Joy Liddicoat for the thoughtful comments. Any errors and responsibilities remain my own.

Table of Contents

1.Introduction

The role of intermediaries in global networked communication is ubiquitous. All producers of content on the internet have to rely on the action of some third party–the so called intermediary–in order to reach their recipients. Such intermediation ranges from the mere provision of connectivity, to more advanced services such as a specific type of communication tool or platform. For example, email and blogging space, or the indexing of the content through a search engine, or a human compiled index or directory (also known, collectively, as information location tools).
Because of the substantial impact that the products and services offered by companies or organisations can have on the unfolding of internet communications, they find themselves potentially at legal risk for the communication and distribution of content which they enable. Specifically, they can be held either directly liable for their actions, or indirectly (or "secondarily") liable for the actions of their users. While this can be seen as an unavoidable consequence of the services these intermediaries have chosen to provide, it is important to recognise that such liability can have a significant deterrent effect on their willingness and ability to provide services, and therefore may end up hindering the development of the internet itself. For this reason, legislators around the globe have defined special "comfort zones" for the operation of intermediaries, also known as "safe harbours", limiting the liability of such entities in specific sets of circumstances.
As this background paper illustrates, significant differences exist concerning the subjects of these limitations (Section 2), their scope (Section 3) and their modes of operation (Section 4). Nevertheless, international best practices can be identified that may provide useful guidance for the drafting or the improvement of the current legislation in a number of African countries.

To that end, this background paper addresses the normative context among African Union members informing the main challenges and opportunities in addressing intermediary liability legislation (Section 5). It then draws on the concept of human rights outlined in the discussion of the African context to highlight safeguards that should be included in the intermediary liability regimes (Section 6). This is followed by a brief conclusive summary (Section 7).

2.Defining intermediaries

Intermediary liability is not a peculiarity of internet law. It represents a standard feature in fiduciary relationships governed by employment and insurance law, as well as banking and securities regulation. It was also often invoked in intellectual property (IP) cases even before the internet era concerning a form of intermediation impacting on the commercial use of a product. For example, a number of US copyright cases in the early 20th century revolved around the concept of vicarious liability[1] for landlords who had provided the venue where an infringement (tenants selling bootleg songs) took place.[2] A landmark judgment by the US Supreme Court in 1984 created a safe harbour from contributory liability for copyright infringement for the sale of copying equipment if it was capable of substantial non-infringing uses.[3] Similarly, several US trademark cases since late 19th century concerned the responsibility of generic drug or beverage manufacturers in the sales of their products by retailers as if they were branded products.[4]

[1]"Vicarious liability" refers to those situations where responsibility for indirect infringement is attributed on the basis of the existence on the part of the defendant of the right and ability to control the infringer's acts, combined with the receiving of a direct financial benefit from the infringement. For an illustration of early US case law on the topic, see: *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 306 (2d Cir. 1963)

[2]For example, see: *Deutsch v. Arnold*, 98 F.2d 686 (2d Cir. 1938); *Fromott v. Aeolina Co.*, 254 F.2d 592 (S.D.N.Y. 1918)

[3]*Sony Corp. of America v. Universal City Studios, Inc.,* 464 U.S. 417 (1984)

[4]These cases were grounded upon theories of contributory liability for having induced or not having interrupted the infringement of a retailer whom they knew or had reason to know was engaging in trademark

In this commercial context, intermediaries are defined as entities functioning as means of communication between different actors helping them to make an agreement.[5] However, in the context of internet governance, this definition needs to be adjusted to refer to the *provision of services* that enable *internet communication* between different users. In other words, a proper definition for our purposes recognises both the purposive character of the servicethat is offered to internet users (either pursuant to a long-term contract or via a one-off transaction) and the fact that the ultimate action that is sought by the customers of these intermediaries is the accomplishment of a communicative act: it enables them to connect to the internet, or to engage in some particular form of networked communication (including for the mere purpose of sale, transmission or distribution). It is the liability of this type of intermediaries that this background paper is intended to address. Specifically, the subject of this paper is intermediary liability in a narrow sense, referring to the "indirect" or "secondary" liability of such intermediaries for the content generated or distributed by their users, and not to the "direct" or "primary" liability for the violation of obligations on the intermediaries themselves (such as, for instance, those regulating the interception of communications or the security of the services provided).
Drawing a comprehensive list of third parties which may be involved in the processing of internet communication can be a daunting and lengthy exercise. However, a few representative categories can be identified:

- *Network operators, mobile telecommunications providers, and access providers, generally known also as internet service providers (ISPs) in the narrow sense*
- *Website hosting companies, including portals, dedicated server space and domain name registrars*
- *Information location tools and content aggregators*
- *E-commerce platforms and online marketplaces*
- *Providers of online services, such as email and cloud providers, which allow user-to-user communications or host user-generated content*
- *Network-related software and applications developers, such as companies designing browsers, anti-virus programs and filtering technologies.*

Internet intermediaries in the US

The leading reference for the identification of different types of intermediaries is the US Digital Millennium Copyright Act of 1998, and in particular section 512, which provided 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 and other international references, safe harbours generally cover three types of intermediation:

- Communication conduits
- Content hosts

infringement. For example, see: *Societe Anonyme de la Distillerie de la Liqueur Benedictine de l'Abbaye de Fecamp v Western Distilling Co*., 42 Fed. Rep. 96 (C.C.E.D.Mo. 1890); *Hostetter Co. v Brueggman-Reinert Distilling Co*., 46 Fed. Rep. 188 (C.C.E.D.Mo. 1891); *Coca-Cola Co. v Snow Crest Beverages, Inc*., 64 F.Supp. 980, 989 – 990 (D. Mass. 1946), aff 'd, 162 F.2d 280 (1st Cir.), cert. denied, 332 US 809, reh'g denied, 332 US 832 (1947*). Inwood Labs, Inc. v Ives Labs, Inc*., 456 US 844 (1982)

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

- Search service and application service providers[6].

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 initiated by the user and directed to the designated recipient(s). This must be done through automated process without any modification or selection of the content or of the recipient, and 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"). Caching is generally done to overcome network connectivity issues and guarantee a ready and speedy access to content. However, this section can be applied not only to ISPs in a narrow sense, but more generally to a number of providers of technical and functional services which improve the experience of communication on the internet.[7] It too defines a safe harbour and requires for that purpose that the content not be modified, and for the service provider to 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.[8] 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 it removed.

It should be noted that caching is not specifically addressed by all intermediary liability regimes, and it is often covered by a more generic formulation of the "conduit" exemption (for instance, in

[6]Organization for Economic Cooperation and Development *The Economic and Social Role of Internet Intermediaries* (Paris: OECD, April 2010), http://www.oecd.org/internet/ieconomy/44949023.pdf

[7]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)

[8]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 is not in line with industry standards and communication protocols.

Canada[9]) or by a broad exemption for intermediaries based on knowledge of illegality (for instance, in China[10], Japan[11] and South Korea[12]).

Content Hosts

Section 512(c) is devoted to a different type of storage 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 from safe harbour only if the provider:

- 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.
- 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.
- 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).

Search Service and Application Service Providers

The next 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 fulfilled by service providers to benefit of this safe harbour are identical to those imposed by section 512(c).

Nonprofit Educational Institutions

The last category of intermediary is described by section 512(e) as "Nonprofit Educational Institutions" that act 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[13], 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

[9]See: Copyright Act of Canada, R.S.C., 1985, c. C-42, s.2.4 (1) b (1985)

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

[11]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, (2001). For an unofficial translation, see: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/H13HO137.pdf

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

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

service described therein can be accommodated through the other safe harbours,[14] it should be acknowledged that its inclusion into the safe harbours 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.

Other intermediary liability rules in the US

Evidently, 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 scenarios, including potential violations in other areas of IP, are dealt with by a general norm in section 47 U.S.C. 230, introduced with the Communication Decency Act (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.*[15]

Finally, the picture on online intermediary liability in the US would be incomplete without mentioning section 32(2) of the Lanham Act, which shields publishers of a periodical 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.[16] This safe harbour 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.[17]

The resulting patchwork arrangement has been criticised for lack of consistency, due to the possibility for plaintiffs to characterise 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 harbour.[18] Lemley also laments a loophole in the existence of a carve-out from the safe harbours for hosting and information location tools, where they require that service providers "[do] not receive a financial benefit directly attributable to the infringing activity, in a case in which [they have] the right and ability to control it." He reads this provision as reflecting the requirements for vicarious liability, which he finds problematic due to the relative ease of making a successful vicarious infringement case under the existing case-law. Although Lee convincingly rejects this view on the basis of both the legislative history of the statute and the difference between the more exacting notion of "financial benefit directly attributable" used in the

[14]By contrast, online activities provided by public educational institutions are explicitly excluded from the scope of the EU Electronic Commerce Directive of 2000, since this is applicable only in relation to information society service providers and information society service required to be "normally provided for remuneration." See: *infra* note 22.

[15]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: Filter, screen, allow, or disallow content; Pick, choose, analyze, or digest content; or transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

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

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

[18]Mark Lemley "Rationalizing Safe Harbors" *Journal of Telecommunications and High Technology Law* 6 (2007): 101-109

statute and the less strict condition of "direct financial interest" referred to in the case-law on vicarious infringement,[19] it seems advisable for legislators to leave out from intermediary liability rules this particular requirement and the confusion that it generates. As to Lemley's other suggestion of standardising safe harbours so as to provide consistency across different areas of law, one needs to look no further than the adoption of the European Copyright Directive 2000/31 (ECD) to find a term of comparison. Accordingly, we shall now turn to examining the ECD, highlighting its drawbacks and strengths.

Internet intermediaries in the EU

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[20], 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.[21]*

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 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 a 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."

Communication Conduits

Article 12 of the directive refers mainly to internet access providers 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 ECD 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.[22]

Article 13 deals with caching, defining it in a much similar way as 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." For purposes of the safe harbour, it requires 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

[19]Edward Lee "Decoding the DMCA Safe Harbors" *Columbia Journal of Law & the Arts* 32, 3 (2009): 233

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

[21]See art. 2 (a) of the European E-Commerce Directive 2000/31, referring to the definition in art. 1(2) of Directive 98/34, as amended by Directive 98/48

[22]EU Commission *EU study on the Legal analysis of a Single Market for the Information Society. New rules for a new age?* 6. Liability of online intermediaries (Brussels: EU Commission, 2009), 14 http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=7022

interfere with the lawful use of technology to obtain data on the use of the information. Moreover, the provider must operate consistent 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 identified by this definition, the EU study noted that it is not entirely clear whether they would encompass decentralised content distribution systems such as Usenet groups and peer to peer networks.[23]

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:

- 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.
- Upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
- Has no authority or control over the recipient.

This is without doubt the most controversial safe harbour of the ECD, for several reasons. First, it does not specify what counts as "actual knowledge", therefore allowing EU member states to adopt different approaches in the implementation of the directive, such as requiring a formal notification by the competent administrative authorities (Spain), the fulfilment of a notice and take-down procedure (Finland), or leaving the determination to national courts on a case by case basis (Germany and Austria). Second, 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.[24]

Third, 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 article 12 of the directive, and Spain, Portugal and Hungary explicitly extending the protections of article 14 (but in the case of Hungary, not to hyperlinks).[25]

[23]Ibid. 15

[24]Ibid. 16

[25]The case of liability for linking is a particularly controversial one across EU member states: for example, Cyprus introduced 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 website to the root site, i.e. to the main portal, so that his interest in earning advertising income can be satisfied by technical means. See OLG Hamburg, 20/.02.2007, 7 U 126/06, available at http://www.suchmaschinen-und-recht.de/urteile/Oberlandesgericht-Hamburg-20070220.html

Internet intermediaries in other legislations

Due to their early adoption and the relative size of the regulated markets, the DMCA and the ECD are the most notorious and looked upon models for intermediary liability around the world. However, other interesting approaches have been adopted with regard to the types of activities that can fall under a safe harbour. One of the most inclusive provisions for the limitation of liability can be found in India's Information Technology Act, where "intermediary," is defined as:

> *…any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.*

The general safe harbour provision[26] establishes that:

> *…no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him, if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.[27]*

Although this model would in principle provide a useful common framework for the "standardisation" of safe harbours, a recent study has found that the lack of a clear definition in the qualifications and due diligence requirements of different classes of intermediaries resulted in significant uncertainty in the steps for them to be followed.[28]

Japan offers another interesting case of uniformisation of all intermediaries, adopting a unique definition of online service provider whose purpose is to communicate third party information to other parties, and establishing a unique safe harbour for secondary liability, based on the actual or constructive knowledge of illegal activity and the necessity of the measure in order to prevent infringements[29]. Likewise, China centers its regime of intermediary liability on the actual or constructive knowledge–although it is debated whether this should be seen as a "should have known" or a "had reason to know" standard.[30]

---

[26]Which applies in addition to, and independently from, the more specific safe harbour for mere conduit activity. See infra note 28

[27]12 Information Technologies Act (2000), Section 79 (emphasis added)

[28]Rishabh Dara "Intermediary Liability in India: Chilling Effects on Free Expression on the Internet" working paper, Indian Institute of Management (IIM), Ahmedabad, 2011. SSRN http://ssrn.com/abstract=2038214 or http://dx.doi.org/10.2139/ssrn.2038214

[29]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

[30]With this general discussion on the standard for tort liability in the backdrop, the State Council's Regulations on Protection of the Right to Communication Through Information Network modified the formulation of the rule for copyright purposes by subjecting the liability limitation to the condition that the service provider "does not know or has no reasonable ground that make him shall have known the infringing content on the system." (Art. 22). This has been read as incorporating both standards, although a clarification in the sense of "should have known" has been provided by the recent Supreme People's Court Provisions on Several Issues Concerning Application of Law in Civil Dispute Cases of Infringing Right to Network Dissemination of Information, See: Qian Tao "Legal framework of online intermediaries' liability in China" *info* 14, 6 (2012): 59-72; Qian Tao "The knowledge standard for the Internet Intermediary Liability in China" *International Journal on Law Information Technology* 20, 1 (2012): 1-18.

Finally, a similar unifying approach to the concept of intermediary, and more specifically of the internet service provider, can be found in article 2.1 of the New Zealand Copyright Act, which describes it as:

A person who does either or both of the following things:

a) offers the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing;

b) hosts material on websites or other electronic retrieval systems that can be accessed by a user.

This definition is in line with the tendency, evident from the safe harbours provided by the great majority of legislations, to distinguish between two broad categories of intermediation: conduits and hosts.

3.Scope of liability

In the preceding section, the scope of liability covered by the safe harbours wasonly mentioned for the purpose of distinguishing "specialist" or "vertical" limitations–like those in the DMCA–from "generalist" or "horizontal" ones–like those in the CDA and the ECD.[31] However, the range of possibilities in the intermediary liability scenario is more complex. This section provides an overview of the two key issues in this respect: liability outside the safe harbours and scope of the safe harbours.

Liability outside the safe harbours

The first important point to be made is that the existence of safe harbours does not imply that an intermediary, upon failing to qualify for it, will necessarily be held liable. In fact, liability will need to be determined in accordance with the applicable law, which may establish additional limitations for particular kinds of conducts, or stringent conditions of correlation between the intermediary's and the defendant's actions. Thus, although the attribution of responsibility is generally based on contributory or vicarious infringement theories, the exact requirements imposed by national statutes or case-law to trigger liability under one of such theories differ.

In the US for example, as noted above, the jurisprudence of the Supreme Court devised in 1984 a safe harbour for the sale of technologies which, even if enabling potential infringements, are capable of substantial non-infringing use[32]. However, more recently the Court narrowed the scope of this safe harbour by specifying that it was never intended to foreclose rules of fault-based liability derived from the common law, and concluding that "Evidence of active steps […] taken to encourage direct infringement, such as advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe, and a showing that infringement was encouraged, overcomes the law's reluctance to find liability when a defendant merely sells a commercial product suitable for some lawful use".[33]

[31]Although the CDA is not applicable to copyright and trademark disputes and does not prevent the enforcement of federal criminal law, this carve-out constitutes merely an exception to the general, horizontal rule. Even the ECD is not entirely horizontal. See, for example, Article1.5 (excluding a number of fields and activities from the scope of the directive)..

[32] *Sony corp. Of Am. V. Universal City Studios, Inc*., 464 U.S. 417, 442 (1984)

[33] *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*., 545 U.S. 913, 936 (2005).

In Germany, in order to make a successful claim of participatory liability, the requisite intent with regard to the unlawful action can only be imputed to the intermediary in the presence of "gross and consistent breach of the obligation to examine an alleged infringement."[34] However, the jurisprudence of the Federal Court of Justice has recently found the duty of intermediaries to "take all technically and economically reasonable measures to prevent future uploads of files which have been reported to be illegally distributed through its service[35]". In Italy, courts expect a proactive stance by the provider in the presence of possible infringement, holding it liable when:

> *…it does not merely provide a connection to the internet, but offers additional services (for example, caching or hosting) and/or monitors information, in particular when it is aware of the existence of suspicious material, does not ascertain its illicit nature and remove it or is aware of the unlawful material and does not act to remove it.[36]*

In the Netherlands, where there is no specific distinction between direct and indirect liability, emphasis is placed also on factors other than actual or imputed knowledge and ability to control, such as: whether there had been active involvement in the publication of illegal material; encouragement of the publication of illegal material either by incitement or by the way the site is organised; and profit through the infringing activity.[37]

The new Tort Liability Law in China[38] provides an example of divergence between general tort law and conditions for the qualification of "vertical" safe harbours: in a specific article for cybertorts (article 36), generally known as the "Internet Clause", the law applies a more lenient standard of knowledge than that used as a condition for the copyright safe harbour ("knew" as opposed to "knew or should have known" or "had reason to know").[39]

In general, in the EU there seems to be a common trend to infer knowledge or awareness upon proof of *manifestly* or *obviously unlawful* content.[40] However, the exact terms of "manifest or obvious unlawfulness" are far from settled: for example, an Austrian court dealing with trademark infringements and business defamation held that the former could not be qualified as being obvious to a non-lawyer, but the latter was.[41] Similarly, the Court of Appeal of Paris qualified as "manifestly illicit" all racist, anti-Semitic or revisionistic content as well as texts which excuse crimes of war, paedophilia or pornographic pictures and contents.[42]

A more convoluted criterion appears to have been devised in Czech Republic and Slovakia, where it is reported that the assessment of the information which the provider is aware of is based on the following principles:

---

[34]LG München, Urt. v. 11.01.2011, *Az.*: 21 O 2793/05 - MMR, 2006, 332, 334f. See also BGH, GRUR 2008, 702 – *Internetauktion III.*

[35] : Bundesgerichtshof, I ZR 18/11 of 12 July 2012, *Alone in the Dark*; I ZR 80/12 of 15 August 2031, *Rapidshare*.

[36]Tribunale di Milano, Sentenza 15 settembre 2011, n. 10893/2011, *Reti Televisive Italiane S.p.A. c. Yahoo! Italia S.r.l.*

[37]LJN: BN1445 & LJN: AU4019

[38]The Tort Law of the People's Republic of China, Decree of the President of the People's Republic of China (No. 21) of December 26, 2009, available at http://www.wipo.int/wipolex/en/details.jsp?id=6596

[39]The article holds internet service providers jointly liable with infringing users if they had knowledge of the illegal activity and failed to take measures expeditiously.

[40]Thibault Verbiest et al. *EC study on the Liability of Internet Intermediaries* (Brussels: European Commission, 2007): 37

[41]AU8. - OLG Innsbruck, 24/5/2005, 2 R 114/05i, http://www.internet4jurists.at/entscheidungen/olgi_114_05i.htm

[42]Conseil Constitutionnel Décision n° 2004-496 DC - 10 juin 2004. http://www.conseil-constitutionnel.fr/decision/2004/2004496/index.htm

- If the information violates public (imperative, absolute) laws such as criminal law, the provider is obliged to reveal its illegality proactively
- If the information infringes individual private (relative) rights, the intermediary is not to be expected to reveal this proactively.[43]

The picture is further complicated by the fact that in some countries, the right itself is defined in such a way that it can be interpreted to cover both the acts of speech by users and the mere automated processing by intermediaries. This is often the case with regard to data protection and copyright legislation.

For example, three Google executives were initially found criminally liable in Italy[44] (a decision eventually reversed by the Italian Supreme Court)[45] for allowing the distribution by one of its users of a video containing sensitive personal information of a third party, without obtaining the latter's consent as required for "data controllers". The issue of the scope of a provider's liability under EU law for processing of personal data is currently under consideration by the European Court of Justice in the *Google Spain* case, in the context of which the Advocate General has expressed the opinion that a search engine provider is not "aware" of the existence of personal data when processing them for the purpose of crawling, analysing and indexing, but is deemed to have such awareness when determining how the index is structured[46]. The breadth of the statutory definition of (direct) copyright infringement can also prove problematic: in the UK, for example, "Copyright in a work is infringed by a person who without the licence of the copyright owner does, *or authorizes another to do*, any of the acts restricted by the copyright."[47] Long-standing case law has interpreted authorisation to mean "sanction, approve and countenance"[48] and a distinction has been made with the concept of enabling, assisting or even encouraging an illegal act without purporting to have any authority to justify the doing of the act."[49] However, a recent case establishing liability of an information location tool under this test indicates that the provision is still perceived a potential threat to the conduct of intermediaries.[50]

In Australia, the Copyright Act contains an equivalent provision,[51] and the high court has clarified in a leading case that "inactivity or indifference, exhibited by acts of commission or omission, may reach a degree from which an authorization or permission may be inferred."[52] More recently, the act has been modified[53] to include, among other things, a test establishing the factors to be taken into account in assessing the existence of an authorisation.[54] The amendments included a

[43]Verbiest et al. *EC study on the Liability of Internet Intermediaries* 40

[44] Tribunale di Milano, sez. IV pnale, sentenza 1972/2010 of 12 april 2010, *Vividown*

[45] Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – 3 febbraio 2014, n. 5107(holding that "the defendants are not data controllers of any data and the sole data controllers of the sensitive data contained in the videos uploaded on the site are the users themselves that uploaded them and against whom the criminal and administrative sanctions prescribed by the Privacy Code can be applied").

[46] Opinion of Advocate General Jääskinen, Case C-131/12, paras. 84-91

[47]UK Copyright, Designs and Patents Act of 1988, section 16 (emphasis added)

[48]*Falcon v. Famous Players Film Co.,* [1926] 2 K.B. 474, 498-499 (C.A. Eng.) (Atkin L.J.), subsequently approved in *CBS Songs Ltd. v. Amstrad Consumer Elec. Plc.,* [1988] A.C. 1013, 1055 (H.L.) (Eng.) (Lord Templeman).

[49]*CBS Inc. v. Ames Records & Tapes Ltd*., [1982] Ch. 91, 106 (Eng.).

[50]*Twentieth Century Fox Film Corp. v. Newzbin Ltd*, [2010] EWHC 608 (Ch), [2010] All ER (D) 43 (Apr), (Eng. Chancery Div.).

[51]Australian Copyright Act, section 13.2

[52]*Moorhouse v. Univ. of N.S.W*., (1975) 133 C.L.R. 1, [1976] R.P.C. 151 (High Ct. Austl.)

[53]Copyright Amendment (Digital Agenda) Act 2000

[54]"(a) the extent (if any) of the person's power to prevent the doing of the act concerned; (b) the nature of any relationship existing between the person and the person who did the act concerned; (c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person

clarification that the internet service provider's enablement of legal acts for its users would not trigger the notion of authorisation,[55] but subsequent decisions demonstrated the persistence of a broad understanding of this notion, holding liable a portal site[56] and the developers and distributors of a peer-to-peer software[57] for not having designed their system in a way that would prevent copyright violations more effectively.

A similar conception of copyright is also in place in Canada, South Africa and Jamaica. In all such countries, it can be argued that the existence of safe harbours to the relevant intermediaries is even more valuable from a legal certainty standpoint. However, as noted above, this circumstance alone does not allow the courts to dispense with the infringement analysis based on the identification of the infringing act(s) and the requisite intent. For this reason, it seems advisable for legislations to include both an acknowledgement in this sense, and a clear test for the level of knowledge or awareness of illegal activity that triggers positive obligations on different kinds of intermediaries.

Scope of the safe harbours

The second important remark on the scope of safe harbours is that liability shields can be of three different types:

- From civil liability in the sense of monetary damages, but excluding injunctive relief[58]
- From civil liability, including certain forms of injunctive relief
- From criminal liability, in addition to one of the above.

The first type of liability shield is the one provided by section 230 of the Communication Decency Act. This is, arguably in light of its pioneering role, the simplest kind of liability limitation: exemption with regard to all kinds of liability (for good faith editorial choices), with the noted exceptions including federal criminal law. It should be noted that this section is currently under the spotlight, as 47 state attorney generals sent a letter to the US congress requesting the expansion of this carve out to include all state criminal laws, which has been perceived by many as a threat to free speech on the internet.[59] Moreover, the absence of a provision clarifying whether these safe harbours also entitle to immunity from injunctive relief has been recently interpreted by the Court of Appeal for the 7th Circuit as a signal in the affirmative, even in the face of an adjudicated proceeding establishing the illegal nature of the material.[60] This is clear evidence of the need for legislators to clarify such matters.

The second liability shield can be described as the most common situation in the modern attempts to regulate online intermediaries: recognising the importance of leaving open the possibility for

complied with any relevant industry codes of practice." See sections 36(1A) and 101(1A) of the Copyright Act.

[55]Section 112E provides that a person "who provides facilities for making, or facilitating the making of, a communication is not taken to have authorized any infringement of copyright in an audio-visual item merely because another person uses the facilities so provided to do something the right to do which is included in the copyright."

[56]*Universal Music Austl. Pty. Ltd. v. Cooper*, [2006] FCAFC 187, [41], [62]-[64] (Fed. Ct. of Austl.)

[57]*Universal Music Austl. Pty Ltd. v. Sharman License Holdings Ltd*, [2005] FCA 1242 (Fed. Ct. of Austl.)

[58]Injunctive relief refers to the obtaining of a court order (an "injunction") consisting of a prohibition against an act or a condition. The prohibition can be either applicable to all future conduct of the recipient, or, most commonly, limited to a predetermined period of time.

[59]Matt Zimmermann "State AGs Ask Congress to Gut Critical CDA 230 Online Speech Protections" (Electronic Frontier Foundation 24 July 2013) https://www.eff.org/deeplinks/2013/07/state-ags-threaten-gut-cda-230-speech-protections

[60]Blockowicz v. Williams, 630 F.3d 563 (7th Cir. 2010).

courts to order a service provider to help in stopping infringements, but at the same time preventing the imposition of an excessive burden on intermediaries. Several legislations make a point in setting limits and conditions to the use of injunctions. This is the case, for example, with regard to section 512 of the DMCA which lists the factors to be considered by courts in granting injunctions.[61] It sets two different types of rules for injunctions depending on whether it targets an intermediary performing mere conduit activity, or one engaged in the other activities listed in sections 512(b) to (e).[62]

The situation is less clear-cut in Europe, where member states have discretion in the implementation of the framework identified by the ECD. Thus, although all countries must respect the general limit in article 15 of the ECD of not imposing on intermediaries general obligations to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity, they are also allowed to use injunctions, as well as legislation, to impose obligations of notification of illegal activity or identification of users.[63]

The third liability shield is a model that is followed by the majority of EU countries using the discretion left by the ECD for the purpose of extending safe harbours to criminal liability. It should be noted that while a safe harbour is always a welcome sign of certainty, the "added value" of an immunity from criminal liability appears less significant in this context than its civil counterpart because the requirement of knowledge to be satisfied for purposes of criminal intent is generally more demanding than the generic knowledge or awareness that can be relied upon in a non-criminal setting. In other words, it is likely that an intermediary, even if does not qualify for the safe harbour, will be able to escape criminal liability in the absence of very clear evidence of intent to participate in the illegality. Nonetheless, it should be borne in mind that the threat of criminal liability can generate substantial chilling effects, and thus where the limits for such liability aren't narrowly defined, a safe harbour allows intermediaries not to be deterred in the first place from potentially beneficial activity.

Perhaps cognisant of the importance of the different standards of proof and the confusion that their interaction with safe harbors can generate, a number of EU states (such as Portugal, Italy, Germany) explicitly distinguish actual knowledge, which can be actionable for criminal purposes, and mere awareness of the circumstances from which the illegal activity or information is apparent,

[61]17 U.S.C. Section 512(j)(2)

[62]In particular, in the first scenario a court can grant injunctions only in one or both of the following forms:
"(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States."
See: U.S.C. Section 512(j)(1)(B)
For all the other safe harbours, the following injunctive relief is available:
"(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.
(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose." See: U.S.C. Section 512(j)(1)(A)

[63]Article 15.2 provides that: "Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

which satisfies the lower threshold of civil liability.[64] Other countries, such as Malta, plainly restrict the liability limitation to civil liability.[65]

Once again, a reference can be made here to India's Information Technology Act to mention one peculiarity that may be useful to resolve the conflict between specific intermediary liability rules, and more stringent general liability standard. Section 81 provides indeed for a "non-obstante" clause, according to which "The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force." A similar clause in the EU could have the practical effect of allowing courts, in case of doubt, to adopt the interpretation more favourable to the intermediary, in accordance with the protective purpose of the liability limitations.

4.Mode of operation

This section schematically describes the dynamics of cooperation between intermediaries and law enforcement. In a recent report, the OECD identified four types:[66]

- Notice and takedown (NTD)
- Notice and notice (NN)
- Notice and disconnection (ND), or the less drastic " graduated response regime"
- Filtering and monitoring, either by mandatory blocking required to the ISP with respect to selected content, or by requiring ISPs to conduct monitoring to identify potentially illegal activity and alleged infringers.

Notice and Takedown (NTD)

NTD systems generally require hosting companies and selection intermediaries to act expeditiously to remove content which it is claimed to be illegal once they have been given notice of the content (for example, section 512 of the DMCA). The provisions laying out the conditions for the safe harbour also require the designation of an agent for the reception of notification, and specify the level of detail that such notifications must have; furthermore, they require the claimants to self-certify (though not under oath) that they have the authority to pursue the claim, and that the information in the notification is accurate. All these rules, as well as the damage liability stipulated by section 512(f) for any knowing misrepresentation of the infringing nature of the activity or of the mistaken nature of the removal or disablement of content, are important components for the operation of the notice and take-down regime.

The actual rules of such regime are contained in section 512(g), which starts by conferring the intermediaries immunity "for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent." However, in contrast to the immunity outlined in section 230 of the Communications Decency Act, this immunity concerns only editorial choices with negative impact on free speech–taking down–as opposed to choices with adverse consequences for those rights of the claimants which are subject to balancing against free speech such as copyright, privacy or defamation rights. In other words, an intermediary may well be

[64]Verbest et al, 34

[65]Malta: § 21 Electronic Commerce Act (Chapter 426) of 10 May 2002 (Act No. III of 2001, as amended by Act No. XXVII of 2002).

[66]Organization for Economic Co-operation and Development *The Economic and Social Role of Internet Intermediaries* (Paris: OECD, 2010) http://www.oecd.org/internet/ieconomy/44949023.pdf

considered liable for not having offered sufficient protection to these rights holders, but not for having removed or disabled access to the content of internet users. Moreover, the grant of immunity is complemented by specific conditions concerning the way this editorial discretion should be exercised. In fact, section 512(g) establishes the additional steps that one has to follow in order to enjoy the immunity. One must:

- Take reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material.
- Upon receipt of a counter notification described in paragraph (3), promptly provide the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and inform that person that it will replace the removed material or cease disabling access to it in 10 business days.
- Replace the removed material and cease disabling access to it not less than ten, nor more than fourteen, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

Criticism abounds concerning the one-sidedness of this regime. First and foremost, as highlighted above, the immunity goes only in one direction. Likewise, the requested material is taken down by a default, for a period of time which may be significant, thereby immediately impacting on free speech. Furthermore, it is not clear whether copyright owners are required before making their takedown request to consider fair use, which is a doctrine that is designed to ensure the balance between copyright exclusivity and public interest.[67] Finally, it is striking that claimants only need to make a statement concerning the legitimacy of their claims, while defendants must do that under oath for purposes of the counter-notice (thereby risking, in the face of the uncertainty of the determinations, the consequent penalties for perjury and civil damages that can be imposed).

In the EU, as noted, there is no uniform NTD procedure, but a specific NTD procedure has been introduced in some EU countries such as Spain, France, Germany, Finland, Hungary and Lithuania.

Finland has arguably the most comprehensive and balanced regime. First, it provides a specific timeline for each step. Second, a notification triggers not only the immediate takedown, but also a forwarding of the notification to the content producer. The latter can decide to return a plea within fourteen days, in which case the intermediary must put the material back, unless otherwise provided by an agreement between the service provider and the content producer or by an order or decision by a court or by a public authority. Accordingly, the Finnish regime is peculiar for accepting derogation to the standard procedure with regard to content that, due to the relative ease in determining its legality even by laymen and non-lawyers, is not subject to a NTD procedure. On the other hand, both the service provider and the content provider have the right to appeal against the court order within fourteen days from its notification. Finally, it is worth stressing the importance of a provision imposing due diligence on the user filing a counter notice. Even without a specific oath requirement, the law explicitly provides that the content producer is liable to compensate damages caused where he has given false information.

Lithuania offers a particular model of self-assessment by the ISP, which is remarkable for its early involvement of the user, and which also effectively confers the ISP with the power to adjudicate

[67]So far, only one court has responded in the affirmative: see *Lentz v. Universal Music Corp*, 572 F. Supp. 2d 1150, N.D. Cal. (2008)

disputes–a task whose entrustment to a private entity can be undesirable for public interest matters. Once the ISP is notified, it must within one working day send a letter to the alleged infringer, in order to inquire about the veracity of the information received in the notification. If the latter disagrees with the information received, then he or she can provide the ISP with a response within three working days. The ISP will then determine whether the arguments in the response are valid and the facts accurate, and *may* to that end contact the relevant control body[68].

In Japan, a variation, called "notice-wait-and-takedown"[69] has been adopted, whereby the notice and takedown only starts to operate once a week has passed from the forwarding of the notification to the alleged infringer, and no counter-notice has been sent to the ISP.[70] Differently from the Lithuanian model, there is no possibility for the ISP to request guidance (thereby *de facto* delegating the decision)to the relevant control body. On the other hand, a strength of this model is the limitation of the instances in which identifying information is provided by ISPs to complainants upon their request. Although it is lamentable that such information is provided without judicial intervention (once again, the ISP performs quasi-judicial functions), it is worth stressing that the ISP is required to conduct a prior hearing of the infringer (unless unable to locate him or in the presence of exceptional circumstances).[71]

But the danger of leaving public interest determinations to private entities should not be underestimated. For this reason, an important example is given by the new Chilean system of copyright, which requires at all times a decision by the competent authority as a prerequisite to the removal or blocking of content by the ISP.[72] Due to the risk of significantly slower copyright enforcement, a doubt can be cast on whether this type of arrangement, which was only instituted in 2010, would be the best way to balance due process and other interests of the users with those of the copyright holders.[73]

However, at least in principle, the benefits of such model are twofold: not only will the NTD disputes not be subject to private adjudication, but the new law also makes clear the meaning of "actual knowledge" which triggers the duty to act expeditiously for removal or disabling, and which is a very controverted point in virtually all intermediary liability legislations worldwide.[74] This is a welcome innovation which would go a long way in filling the gap of certainty with regard to the standard of conduct which intermediaries must conform to. This uncertainty is particularly significant in the EU, where according to Recital 48 of the ECD, member states may require hosts to "apply duties of care, which can reasonably be expected [...], in order to detect and prevent certain types of illegal activities."

[68] Verbest et al.,108-109

[69]Jeremy de Beer & Christopher D Clemmer "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?" *Jurimetrics* 49, 4 (2009)

[70]See Art. 3 of the 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

[71]Ibid. Article 4 (Demand for Disclosure of Identification Information of the Sender, Etc.) 3

[72]Access *Towards a Rights-Respecting Copyright Enforcement Mechanism: An Alternative to Notice & Takedown* (New York, Access, September 2011): 6 https://s3.amazonaws.com/access.3cdn.net/1a153f88d1ada103f3_1cm6ivbpt.pdf

[73]See in this sense: Center for Technology & Democracy *Chile's Notice-and-Takedown System for Copyright Protection: An Alternative Approach* (Washington: CDT, August 2012) www.cdt.org/files/pdfs/Chile-notice-takedown.pdf

[74]See: Law No. 17336, article 85 Ñ, second subsection: "The service provider shall be understood to have actual knowledge when a competent court, pursuant to the procedure set forth in article 85 Q, has ordered that the data should be removed or that access should be disabled, and the service provider has been legally notified of such order and nevertheless fails to comply with it expeditiously."

The vagueness of that provision, which hasn't been spared from scholarly criticism,[75] not only is dangerous for the predictability needed by intermediaries to operate, but is also worrying for the development of a European single market for electronic communications: the higher standard of care imposed in a particular state may hinder the operations of a national service provider, giving competitors from other member states a competitive advantage.[76]

Notice and Notice (NN)

Canada is a leading example of the second type of dynamic of engagement of intermediaries, the notice and notice (NN) system. A NN system is, in its simplest form, a mechanism which requires an intermediary to forward the notice received by one rightholder to the alleged infringer. What is remarkable about the development of this mechanism in Canada is that it originated as a self-regulatory initiative, in the shadow of the absence of state control over the procedures for the adjudication of online content disputes. As a result of that, the Canadian Association of Internet Service Providers, the Canadian Cable Television Association, and the Canadian Recording Industry Association agreed in 2000 to a voluntary "notice and notice" system[77] whereby internet service providers would simply forward the notifications of infringement from content owners to individual users, and the latter were required to either remove the content or respond within a limited period of time. The system has proven to be a success for its deterrent and educational effect on users, having rarely progressed to the stage of court litigation[78] and has recently been adopted by the state as part of the Copyright Amendment Act, which entered into force in November 2012. According to Section 41.25(1) of the Copyright Act, a notice of claimed infringement can be sent to a person who provides:

- The means, in the course of providing services related to the operation of the Internet or another digital network, of telecommunication through which the electronic location that is the subject of the claim of infringement is connected to the Internet or another digital network.
- For the purpose set out in subsection 31.1(4), for example "hosting," the digital memory that is used for the electronic location to which the claim of infringement relates.

To ensure a smooth functioning of this regime, section 41.26(3) provides the possibility of applying to court to impose statutory damages in an amount of no less than CAD 5,000 (USD 4,973 at time of publication) and no more than CAD 10,000 (USD 9,846 at time of publication). On the other

[75]Rosa Julia-Barcelo and Kamiel J Koelman "Intermediary Liability in the E-Commerce Directive: So far so good, but it's not enough" *Computer Law & Security Report* 16, 4 (2000): 232; Christoph De Preter "Wie heeft nog boodschap aan de boodschap? De aansprakelijkheid van tussenpersonen onder de Wet Elektronische Handel" *Auteurs & Media* 4 (2003): 265-266; Etienne Montero "La responsabilité des prestataires intermédiaires sur les réseaux" in *Le commerce électronique européen sur les rails?* (Brussels: Bruylant, 2001), 289

[76]A case in point is reported to have occurred in Germany, where it has been held the German Federal Court of Justice (Der Bundesgerichtshof) held in a series of cases that eBay, having knowledge of the fact that a particular seller had infringed trademark law, was found responsible for not having taken measures to prevent further infringements, if such measures were possible and economically reasonable. See: *Rolex v Ebay/Ricardo (Internet Auction I)* BGH 11.03.2004, I ZR 304/401, JurPC Web-Dock; Peter Leonard "Safe Harbors in Choppy Waters – Building A Sensible Approach to Liability of Internet Intermediaries in Australia" *Journal of International Media & Entertainment Law* 3, 2 (2011): 221; Broder Kleinschmidt "An International Comparison of ISP's Liabilities for Unlawful Third Party Content" *International Journal of Law and Information Technology* 18, 4 (2010)

[77]Amanda Carpenter, "Bill C-32: Clarifying the Roles and Responsibilities of Internet Service Providers and Search Engines" (IP Osgoode, 15 June 15, 2010) http://www.iposgoode.ca/2010/06/bill-c-32-clarifying-the-roles-and-responsibilities-of-internet-service-providers-and-search-engines/

[78]Gregory R Hagen "Modernizing ISP Copyright Liability", in *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda* Michael Geist, ed. (Toronto: Irwin Law, 2010), 359-360

hand, this damages action is the only remedy for content owners against the inaction of ISPs, as the same section rules out the use of injunctions to compel compliance. Nonetheless, the possibility remains for content owners to resort to court proceedings outside the NN system, where they can subpoena ISPs to obtain the identity of the infringers. As a result, the advantage of this system, which has also been recently adopted as code of conduct by Swiss internet providers[79] and proposed as part of the reform of the UK Defamation law[80] is that it allows individuals to take down content without court proceedings being initiated, their identity being revealed or liability imposed. This is particularly effective considering that users, especially the younger ones, are not always aware of the illegality of their actions.

Notice and Disconnection (ND)

The third model of intermediary involvement is one called notice and disconnection (ND), and is again the evolution of an industry-driven initiative[81] aimed to crack down on copyright infringement by targeting the so called "repeat infringers" through a system of graduate response, comprising different types of sanctions depending on the extent of recidivism of the alleged infringer. The basic mechanism involves a first notice which is merely informative, and contains a series of steps in case of repetition of infringing activity within a specified period of time (usually one to three years), up to the slowing down or termination of the internet connection. Yet, the exact details of how graduated response regimes operate vary. By way of example, the first graduated response law– the French HADOPI law (also called the "three strike law" due to the number of steps involved), culminated with the imposition of a sanction of suspension of internet access for a period of two to twelve months, and was administered by an administrative authority without any judicial oversight. For this reason, the French Constitutional Court found unconstitutional its operative provisions on the ground that they violated the principles of freedom of expression, presumption of innocence and due process.[82]

A similar administrative system was recently introduced in South Korea, charging the copyright commission with the task of recommending ISPs to terminate particular subscriber accounts, and granting the minister of culture, sports, and tourism with the power to order the same.[83] Although the minister has never ordered suspensions, the high rate of compliance by ISPs with the commission's recommendations[84] suggests that the apparent voluntariness of the scheme devised

[79]ILO "Swiss Internet Industry Association adopts hosting code of conduct" (International Law Office, 6 August 2013) http://www.internationallawoffice.com/newsletters/detail.aspx?g=8562998b-1b0e-41cb-955f-03147d7c943f

[80] See: Daithi Mac Sithigh "The fragmentation of intermediary liability in the UK" *Journal of Intellectual Property Law & Practice* 8, 7 (2013): 521-527, noting however less favourably the inclusion of the possibility to obtain the identity of the individual users during the notice and notice process.

[81]For an illustration of the birth of this mechanism in France and the UK, see: The Olivennes Commission *The "Élysée Agreement" for the Development and Protection of Creative Works and Cultural Programmes on the New Networks* (Paris; 23 November 2007) http://www.culture.gouv.fr/culture/actualites/dossiers/internet-creation08/Accords_Fiche_explicative(anglais).pdf See also, most recently, the endorsement of the ISP's "five strikes" plan by US Intellectual Property Enforcement Coordinator: Victoria Espinel "Coming Together to Combat Online Piracy and Counterfeiting" (White House Office of Management and Budget blog, 15 July 2013) http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting

[82]*Loi favorisant la diffusion et la protection de la création sur internet,* Conseil Constitutionnel, Décision n° 2009-580 DC du 10 juin 2009. It should be noted that following the ruling of unconstitutionality France passed an amendment requiring a judicial determination before any decision terminating an internet connection.

[83]Pursuant to articles 133 bis and ter of the Korean Copyright Act, see: Heesob Nam "Facts and Figures on Copyright Three-Strike Rule in Korea" (Heesob's IP Blog, 24 October 2010) http://hurips.blogspot.com/2010/10/facts-and-figures-on-copyright-three.html

[84]In the first full year of the scheme's operation, no ministerial order to suspend a subscriber account was made, but 31 recommendations to suspend subscriber internet access were made by the commission and complied with by ISPs. Ibid.

to determine suspensions would not be a valid excuse for exonerating the state from responsibility for any violation of due process and freedom of expression.

There appears to be a trend for legislators to consider a graduate response framework following the establishment of a NN regime. For instance, another "three strike" framework was recently introduced in New Zealand through an amendment of the Copyright Act, the Copyright (Infringing File Sharing) Amendment Act 2011, establishing a notice-based regime where copyright owners provide ISPs with allegations of copyright infringement identified by IP address, and ISPs forward individual notices to the subscribers associated with those IP addresses. Once an ISP has forwarded three notices within a nine-month period to the same user, it will provide anonymised account of that to the relevant copyright owner, which can then decide to apply to the copyright tribunal for an order of damages up to NZD 15,000 (USD 12,345 at time of publication), or to the district court for a suspension of internet access for up to six months. However, following a recommendation of the parliamentary commerce committee, it was decided that the termination provision would only be brought into effect once sufficient evidence is available that the "notice and notice" system and the tribunal-imposed penalties are not sufficient to deter infringement.[85]

A similar regime has been envisaged by the UK's Digital Economy Act, which, besides introducing the "notice and notice" regime, requires ISPs to provide copyright owners (upon request) with anonymised reports showing numbers of notices received by each subscriber, and allows copyright owners to apply for a court order to reveal the names and addresses of subscribers on the list. The act also provided for the future introduction of a graduated response scheme through a code of practice administered by Ofcom (The UK's communications regulator) and with a dispute resolution mechanism requiring both substantial user involvement and a robust and effective appeals mechanism. Ofcom initiated, to that end, a multi-stakeholder consultation process on a first and a revised draft "initial obligations" code.[86]

While the fulfilment of the promises of openness, multi-stakeholderism and incorporation of sufficient safeguards will have to be tested with the final adoption of the code, it should be noted that the existence of arrangements among ISPs to penalize repeated infringers appears to increasingly be the rule, rather than the exception, in copyright enforcement regimes. In fact, one of the conditions for ISPs to enjoy the safe harbours established by the DMCA (and exported around the world through US trade agreements) is specifically that they adopt and reasonably implement a policy for the termination of the accounts of repeat infringers.[87]

An identical condition was introduced into the Australian Copyright Act (section 116 AH) as part of the Copyright Amendment Act of 2006 (which made changes required by the US-Australia Free Trade Agreement)[88] and represents a standard feature in modern US free trade agreements.[89] This, in combination with the history of the DMCA, shows the correlation between the increasing diffusion of graduated response regimes and the US copyright lobby pushing both domestically and

[85]Copyright (Infringing File Sharing) Amendment Act 2011 (NZ), s 122R.
Nicolas P Suzor and Brian F Fitzgerald "The legitimacy of graduated response schemes in copyright law" *University of New South Wales Law Journal* 34, 1 (2011)

[86]Thomas Dillon "United Kingdom" (GraduatedResponse.org) http://graduatedresponse.org/new/?page_id=26

[87]Section 512(i)

[88]House of Representatives, The Parliament of the Commonwealth of Australia, Copyright Amendment Bill 2006. Explanatory memorandum: available at http://www.austlii.edu.au/au/legis/cth/bill_em/cab2006223/memo_0.html

[89]See, by way of example, the free trade agreements with Singapore http://www.cptech.org/ip/health/c/singapore/ussfta-ipr-chapter.html and Chile http://www.sice.oas.org/tpcstudies/uscaftachl_e/Matrix17.htm

internationally for their adoption as a necessary tool to fight piracy. Yet, recent scholarship has criticised the assumption that such regimes would be necessary or effective in accomplishing that objective.[90]

Filtering

The last type of intermediary involvement is one of monitoring and/or filtering. In this respect, it is useful to recall section 512(i) of the DMCA, which, in addition to requiring the adoption and implementation of a system to terminate repeat infringers, requires that the ISP "accommodates and does not interfere with standard technical measures," where "standard technical measures" means "technical measures that are used by copyright owners to identify or protect copyrighted works. These measures must respect the following conditions:

- Have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process
- Be available to any person on reasonable and non-discriminatory terms
- Do not impose substantial costs on service providers or substantial burdens on their systems or networks.

Clearly, this provision grants states some leeway which can be used to impose a certain degree of filtering or monitoring, provided that it is in accordance with industry standards.[91] The imposition of monitoring obligations is however limited by section 512(m), which makes clear that the conditions of the safe harbours cannot be construed to require "monitoring or affirmatively seeking facts indicating infringing activity." Nonetheless, it is lamentable that this section specifies that standard technical measures developed in accordance with section 512(i) can legitimately derogate from such limits, thereby conferring exceeding discretion for the implementation of industry-wide mandates.[92]

In comparison, the provision in article 15 of the ECD, according to which service providers have no general obligation to monitor communications on their networks, is more of an effective safeguard of the freedom of communication against potential industry lobbying. However, it should be noted that whereas section 512 explicitly regulates the issuing of injunctions with regard to mere conduits,[93] the ECD merely indicates in article 12.3 that the article does not prevent the possibility for a court to require the ISP to prevent an infringement. Accordingly, it has been argued that while in the US the industry turns to the legislature, in the EU it will turn to the judiciary so as to give practical content to the rather general provisions of the law.[94] All in all, despite the relative

[90]Annemarie Bridy "Graduated Response American Style: 'Six Strikes' Measured Against Five Norms" Fordham Intellectual Property, Media & Entertainment Law Journal 23, 1 (2012): 1-66; Rebecca Giblin "On the (new) New Zealand graduated response law (and why it's unlikely to achieve its aims)" *Telecommunications Journal of Australia* 62, 4 (2012): 54.1-54.14; Rebecca Giblin "Evaluating Graduated Response" Columbia Journal of Law & the Arts forthcoming (Posted at SSRN on 14 September 2013): http://ssrn.com/abstract=2322516 or http://dx.doi.org/10.2139/ssrn.2322516

[91]Once again, one could argue that a bias against users illustrates the lamented one-sidedness of section 512, as the process of development of such standards only mentions the participation of ISPs and copyright owners.

[92]See Section 512(m) ("Protection of privacy").

[93]In particular, section 512(j) (B) (ii) allows the ISP only to block access to a particular identified infringer by terminating his account, as well as "*taking reasonable steps to lock access, to a specific, identified, online location outside the United States*". Moreover, section 512(j) (B) (iii) lays out the consideration that courts should take into account when requested to issue injunctions..

[94]Miquel Peguera "The DMCA Safe Harbours and Their European Counterparts: A Comparative Analysis of Some Common Problems" *Columbia Journal of Law & the Arts* 32, 4 (2009): 481

disadvantages of this mechanism (for example, slower process and particularised application), it confirms to be a more effective safeguard against abuse.

A number of recent cases in Europe have brought the issue of filtering and monitoring obligations to the fore, questioning the extent to which ISPs can be imposed such obligations within the limits set out by the directive.[95] Important clarifications were provided by the European Court of Justice through two preliminary rulings in 2011 In *Scarlet*, it ruled that a Belgian court's order to an ISP to implement disproportionate blocking and filtering to prevent illegal downloading would be tantamount to imposing a monitoring obligation in contravention of article 15 of the ECD.

Specifically, the court noted that forcing ISPs to implement filter systems, installed at the ISP's own expense and used for an unlimited period of time, would breach the ISP's rights to conduct business freely, as well as infringe on individuals' rights to privacy and personal data protection.[96] In *L'Oreal v. Ebay*[97] the Court was asked to clarify, among other things, whether an ISP may be ordered to take measures making it easier to identify its customers, in particular when it does not decide, on its own initiative, to bring to an end infringements of intellectual property rights and to prevent further such infringements. Contrary to its 2008 ruling in *Productores de Música de España (Promusicae) v. Telefónica de España*[98] where it established that European law neither requires nor prevents orders to ISPs to disclose their subscribers' identities for the purpose of civil litigation,[99] the court answered in the affirmative, specifying that "when the infringer is operating in the course of trade and not in a private matter, that person must be clearly identifiable."

One effect of this ruling, which suggests a higher protection for private information of users operating outside the course of trade, is to mark a significant difference with the rules concerning user identification in United States, where a service provider served with a subpoena in this sense shall:[100]

[95]Three examples of injunctions granted against ISPs include:

- A Belgian Court ordering two ISPs to block Pirate Bay: http://www.edri.org/files/piratebay-decision-belgium-2011.pdf (Antwerp Court of Appeal, September 26, 2011)
- A British Court ordering ISPs to block access to Newzbin, a file-sharing site: *Twentieth Century Fox v. British Telecommunications* (High Court of Justice, October 26, 2011), http://www.bailii.org/ew/cases/EWHC/Ch/2010/608.html
- A Dutch Court ordering two ISPs to block Pirate Bay: *BREIN v. Ziggo/XS4ALL* (The Hague District Court case 374634/HA ZA 10-3184, Jan. 11, 2012), http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BV0549.

In contrast with this trend, the High Court of Australia on 20 April 2012 refused to hold that an access provider should be held responsible for having authorised the infringements because it did not terminate the accounts of users who were alleged to be repeat infringers. See: *Roadshow Films Pty Ltd v iiNet Ltd* [2012] High Court of Australia 16 (20 April 2012), available at http://www.afr.com/rw/2009-2014/AFR/2012/04/20/Photos/f5b0c2ee-8a80-11e1-b8f3-89181177a90a___www.austlii.edu.au_au_cases_cth_HCA_2012_16.pdf

[96]Judgment of the Court (Third Chamber) of 24 November 2011. *Scarlet Extended SA v Societé belge*

des auteurs, compositeurs et éditeurs SCRL (SABAM) http://curia.europa.eu/juris/document/document.jsf?docid=115202&doclang=EN&mode=&part=1

[97] *L'Oréal SA and Others v eBay International AG and Others*. European Court of Justice (Grand Chamber) of July 12, 2011, Case C-324/09.

[98]*Productores de Música de España (Promusicae) v. Telefónica de España S.A.U.,* European Court of Justice (Grand Chamber) of January 29, 2008, Case C-275/06

[99]In particular, the court recognised that such an order may be necessary to ensure that there is an effective remedy. See Ibid. at 142. Furthermore, the court held that any injunction that may be necessary to prevent further infringements must be effective, proportionate, and dissuasive and must not create barriers to legitimate trade. Ibid. at 144.

[100]Section 512(h) provides that such subpoenas may be requested to the clerk of any US district court, by filing with him: "(A)a copy of a notification described in subsection (c)(3)(A); (B) a proposed subpoena; and (C)a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title [the Copyright Act]."

> *…expeditiously disclose to the copyright owner or person authorized by the copyright owner the information[...], notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.*[101]

In short, while the DMCA and the ECD specify that general monitoring obligations should not be imposed, both contain language that could be read as requiring the installation of filters for illegal content, and in EU, the release of information identifying users operating in the course of trade. By contrast, in countries where there is no provision ruling out an interpretation that would impose general monitoring obligations, such as China,[102] there is even more uncertainty concerning the extent of monitoring that internet service providers should conduct, which has resulted in both a disincentive for self-regulation and the expectation of a certain degree of human review over user-generated content.[103] This shows that it is necessary for an intermediary liability framework to include both a provision preventing the imposition of general monitoring obligations, and a more specific attribution of rights and responsibilities with regard to the use of filtering technologies.

5.Accounting for the African context

Devising a regime of intermediary liability in Africa requires a legislator to take into account the complex socio-economic and normative framework within which such system would operate. To start, it goes without saying that any such regime shall be built upon the relevant national legal rules and procedures, consistent with each state's constitution and with general principles of law. In particular, it is advisable that the regime does not simply transpose laws taken from other models which have proven successful or are internationally renowned, as such laws may well face implementation obstacles or impose concepts which radically depart from existing sociological and legal rules, if not from specific standards of liability in civil or criminal law.

Ultimately, that could generate problems of inconsistency, misunderstanding and repulsion due to a sentiment of foreignness to the "transplant." This is unfortunately a recurring feature in the African continent, where a significant number of laws have been imposed upon by movements of colonisation. It is at least in part because of this dynamic, that is not uncommon to see laws or constitutions professing the importance of an effective protection of a particular right or value, yet not being fully implemented with flanking or enabling legislation despite specific provisions in this sense.

For example, the South African Constitution of 1996 provided in its section 32 for the "right to access information," including a clause establishing that "National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state."[104] However, this particular provision was not implemented until 2000, when the Promotion of Access to Information Act was enacted. Even more striking is the case of the right to privacy, which was affirmed in article 12 of the constitution but has not found

[101]Section 512(h) (5)

[102]Only a more vague provision on monitoring has been included in the recently adopted (26 November 2012) Supreme People's Court Provisions on Several Issues Concerning Application of Law in Civil Dispute Cases of Infringing Right to Network Dissemination of Information. According to Article 8 of the Provisions:

> *[...]If an ISP fails to actively check infringing activity conducted by its network users, the People's Court shall not determine it to be at fault [...]If an ISP can prove it has adopted fairly reasonable and effective technological measures, in spite of the difficulty in discovering infringement against information broadcasting by networks as conducted by the network user, the People's Court shall determine it to be without fault.*

[103]Qian Tao "Legal framework of online intermediaries' liability in China", 62; Qian Tao "The knowledge standard for the Internet Intermediary Liability in China", 16

[104]Article 32.2 of the South African Constitution of 1996

legislative implementation until August 2013, when the Protection Of Personal Information Bill was finally sent to the President for signature.[105]

Besides these practical concerns, an intermediary liability regime in Africa must ensure the attunement with the regional human rights standard of the region. In particular, it will be crucial to assess the conformity of the liability regime with the articles protecting freedom of expression, privacy and due process.

The primary instrument of reference for this assessment is the African Charter for Human and People's Rights, entered into force in 1986 amongst the members of the Organization of African Unity, then replaced by the African Union (AU). Today, the AU has a total of 54 states parties and 53 have ratified the African Charter for Human and People's Rights.[106]

Differently from their precursors in the preparation of the International Bill of Rights, the European Convention of Human Rights and the Inter-American Convention of Human Rights, the drafters of the African charter did not consider it necessary to insert a list of limitations into the articles concerned with the protection of specific rights. Instead, they opted for a general limitation clause (article 27) applicable to the exercise of all the rights contained in the charter, according to which "The rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest**."**

Although from a theoretical standpoint the lack of calibration of the limiting principles to the specific rights does not present obvious disadvantages for the effectiveness of protection, the argument can be advanced that in practice, the vagueness of this provision is likely to leave enough leeway for states to justify a wide range of restrictions. Moreover, the absence of a "necessity requirement" (as opposed to the tenuous "due regard" link contained in article 27) makes the implementation of those limitations less transparent, and therefore more difficult to challenge for potential victims.

Aside from this structural issue, the charter suffers also from a substantive deficiency when compared to other regional human rights standards for the purposes of laws relating to internet intermediary liability. It does not explicitly recognise a right to privacy or private life. As shown in part by the South African experience, this is a concept that is only gradually making its way into African law, and was not sufficiently established when the convention was signed. In contrast, the Charter contains a thin article on the protection of freedom of expression (article 9), according to which "Every individual shall have the right to receive information" and "Every individual shall have the right to express and disseminate his opinions within the law."

The African Commission on Human and Peoples' Rights, the organ entrusted with overseeing the charter (including by adjudicating complaints lodged by individuals for violation of the charter's rights), adopted in 2002 a Declaration of Principles on Freedom of Expression in Africa which contains an explicit reference to the formula utilised under the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), providing that "Any restrictions on freedom of expression shall be provided by law, serve a legitimate interest and be necessary and in a democratic society."[107] The declaration does not have binding value, but

[105]Hunton and Williams LLP "South Africa Passes Comprehensive Data Protection Legislation" (Privacy and Information Security Law Blog, 30 August 2013) http://www.huntonprivacyblog.com/2013/08/articles/south-africa-passes-comprehensive-personal-data-protection-legislation/

[106]As of October 2013, the only member state that has not ratified the charter is South Sudan. See: http://www.achpr.org/instruments/achpr/ratification/

[107]See Article II of the Declaration of Principles on Freedom of Expression in Africa.

remains an authoritative instrument and according to its article XVI, "State Parties to the African Charter on Human and People's Rights should make every effort to give practical effect to these principles."

Another interesting feature of the declaration is article IX, devoted to the establishment of a complaints procedure for the violation of the right to freedom of expression in print or broadcasting. After recommending that an administrative body be created for that purpose which shall be insulated from political, economic or any other undue interference, but at the same time that it shall not seek to usurp the role of the courts, the article lays out the inspirational principle that: "Effective self-regulation is the best system for promoting high standards in the media."

This statement has no equivalent in any other human rights instrument, and demonstrates both a belief in the capacity of the private sector to provide an effective control mechanism, and a suggestion to adopt a hands-off approach to regulation of this right in the media by the various members of the African Union. Although the potential effectiveness of the private sector in providing a regulatory mechanism in the absence of state action should not be underestimated, it has been already noted above that self-regulation carries with it significant dangers of "contamination" of the public interest, and should therefore be accompanied by adequate safeguards.

Arguably even more authoritative, although still not a binding instrument is the Joint Declaration on Freedom of Expression and the Internet adopted on June 1, 2011 by the 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.

In the joint declaration, the four rapporteurs make a number of interesting points. First, in a section devoted to general principles (section 1), they stress that the specialty of the internet should be taken into account in developing solutions for the treatment of illegal content, and along that line, they suggest (in line with article XI of the Declaration on Freedom of Expression) that self-regulation can be an effective tool in redressing harmful speech, and should be promoted. In a specific section on intermediary liability (section 2), they restate the "mere conduit principle" (as contained in virtually every regime of intermediary liability) and suggest the possibility of limiting the liability of other intermediaries under the same conditions. Finally, and more importantly for our purposes, the rapporteurs warn against the imposition of duties to monitor and against extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (as is the case under several regimes today). This is important because it complements the concepts of self-regulatory mechanisms with the need for safeguards, which a system for intermediary liability in Africa must lay out with clarity.

Other sections of the joint declaration are also relevant, in particular that on civil and criminal liability (section 4) which recommends that the standard of liability take into account the overall public interest in protecting both the expression and the forum in which is made. The section on network neutrality (section 5), which professes the principle and requires transparency about traffic management, is especially relevant in the context of graduated response regimes. Last, but not least, the declaration addresses through the same framework–proportionality and consistency with narrowly predefined legitimate objectives–both filtering and internet access (Sections 3 and 6):with regard to the former, it adds the requirement of transparency of the measures adopted; with

regard to the latter, it emphasises the obligations for states to promote universal access and to justify any interruption of that service in accordance with the above mentioned standards.

Finally, it should be noted that the ACHPR Special Rapporteur on Freedom of Expression and Access to Information has developed, in partnership with the Centre for Human Rights at the University of Pretoria, a Draft Model Law for AU Member States on Access to Information[108] to give more specific content to the right enshrined in article 9.1. Interestingly, the draft refers to a set of principles that apply to both public and private bodies, which would prevent them from rejecting information requests by citizens of AU member countries except for compelling justifications identified in the model law[109] and only provided that the public interest does not override those justifications. This draft model law is not binding on any AU member, but constitutes an important reference for future law drafting. Drawing upon this common reference for AU members, an option would be for African Union members to adopt a regional IIL regime which provides room for national variations, much like the aforementioned ECD. However, the unsatisfactory results of the ECD experience, which have prompted recently the European Commission to propose the adoption of a harmonised NTD procedure,[110] point to the need to regulate several elements of the IIL regime in detail.

After this review of the rights to privacy and freedom of expression, we shall make reference to the article 7.1 which incorporates due process into the charter. This article notes that every individual shall have the right to have his cause heard. This comprises of:

- The right to an appeal to competent national organs against acts of violating his fundamental rights as recognized and guaranteed by conventions, laws, regulations and customs in force
- The right to be presumed innocent until proved guilty by a competent court or tribunal
- The right to defence, including the right to be defended by counsel of his choice
- The right to be tried within a reasonable time by an impartial court or tribunal.

This article is perhaps the best illustration of how central the role of the right to be heard is to the concept of fair trial. It starts with reference to this fundamental right, and then goes on to say that this comprises the above mentioned requirements. The interpretation of this article is closely aligned to the jurisprudence of the United Nations Human Rights Committee, and is inspired by both the Resolution on the Right to Recourse and Fair Trial issued in 1992 and the Guidelines on the Right to Fair Trial and Legal Aid in Africa adopted in 2003 by the commission. However, it has been noted that most of the cases brought to the commission were decided before the adoption of the guidelines and on relatively egregious violations, and thus most of the details of the content of the right to a fair trial constitute uncharted territory.[111]

[108]Draft Model Law for AU Member States on Access to Information: http://www.achpr.org/files/instruments/access-information/achpr_instr_draft_model_law_access_to_information_2011_eng.pdf

[109]Such as: commercial and confidential information (art. 39), protection of life, health and safety of an individual (art. 40), national security and defense (art. 41). international relations (art. 42), economic interests of the State (art. 43); law enforcement (art. 44), legally privileged documents (art. 45), academic or professional examination or recruitment process (art. 46).

[110]See: European Commission "A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries" http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm

[111]Brownen Manby,"Civil and Political Rights in the African Charter on Human and Peoples' Rights: Articles 1-7", in *The African Charter on Human and People's Rights. The System In Practice, 1986-2006* eds. Malcom Evans and Rachel Murray (Cambridge: Cambridge University Press, 2008)

Nonetheless, the African Charter appears to be–at least on paper–more progressive than any other international human rights instrument. The most striking feature is that the presumption of innocence contained therein applies with full force in the non-criminal context as well.

Another interesting element is that the AfCHPR has made clear in its case-law that, although the right to appeal can be satisfied both through a right of access to court and through a right to appeal from a first instance to a higher court[112], the latter occurs only if the appellate court has jurisdiction over both facts and law.[113] This has a direct bearing on the type of structural arrangements that ought to be made in order to allow users to appeal against blocking and removal decisions.

In short, any mechanism devised for the liability of intermediaries in Africa must be consistent with the right to be presumed innocent, the right of access to a tribunal and the right to appeal-even for civil cases Additionally, it must ensure that the measures imposed upon individual users be provided by law, serve a legitimate interest and be necessary and proportionate for the respect of the rights of others, collective security, morality and common interest**.** Finally, although self-regulatory mechanisms such as the development of specific takedown procedures are encouraged, these must include sufficient safeguards against abuse.

6.Safeguards

When examining flaws in the existing models of intermediary liability from the perspective of the requirements imposed by human rights law, it is clear that recommendations for a model liability regime should include a number of safeguards. Accordingly, the following section outlines the potential abuses of a regime on internet intermediary liability (IIL) by each of the categories of subjects that are directly affected by its design, and describes a number of safeguards that can be introduced in that respect.

Complainants

An IIL regime may be exposed to two types of abuses by complainants. First, they may act strategically in response to the incentives that are set out for intermediaries by making unmeritorious claims to have specific content removed, thereby potentially chilling free speech. Second, they may utilise the provisions of the IIL regime to gather personal information about the users, by misrepresenting the facts and obtaining a discovery order prior to the adjudication of the merits of the case.

The first issue can be addressed through the establishment of litigation sanctions, such as section 512(f) of the US DMCA, providing that any person who makes a knowing and material misrepresentation asserting that any material or activity is infringing, or that it was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer and the service provider. In order to ensure the effectiveness of this safeguard, the IIL regime could require claimants to address the validity of common defences to the infringements alleged, such as fair use in the field of copyright, for example by filling out the appropriate blank spaces in a standardised complaint form.

The safeguard to address the second issue is not peculiar to those systems which, like DMCA section 512(h), confer a pre-complaint subpoena power to identify infringers: similar problems

[112]Communications 159/96, 97/93, 27/89,71/92, 49/91 and 99/93

[113]Communications 54/91, 61/91, 98/93, 164/97-196/97 and 210/98, para. 94

arise when there is a procedure in place, like in the Japanese system, where intermediaries adjudicate without judicial oversight disputes possibly leading to the identification of users based on the complainants' likelihood of success on the merits. Accordingly, the safeguards that can address these issues must at a minimum introduce a judicial oversight requirement, so as to ensure independence, impartiality as well as competence of the body making the determination of legality. At the same time, it seems reasonable also to conceive exceptions, such as in the case of "obvious and flagrant" infringements and where the undertaking of a court proceeding would impair the effectiveness of law enforcement. Inspiration may also be drawn from the Czech and Slovak practice of inferring knowledge of illegal material, which distinguished based on the absolute or relative nature of the rights being infringed. Finally, certain limits could be devised to exclude the possibility of revealing specific type of personal information (such as websites visited or search log history) or allowing the identification of users in specific circumstances, for example, when they have acted in a private capacity as opposed to in the course of trade.[114]

Users

Similar to the complainants, internet users may rely on the rules of the IIL regime to "game" the system, for example by asserting unmeritorious defences to keep infringing content online if a counter-notice possibility is provided. In this respect, a litigation sanction such as DMCA section 512(f) would appear sufficient to deter abusive defences. By contrast, the imposition of an oath requirement for the absolute truth of the statements contained in counter notices would appear unnecessary and may result in too strong a deterrent, particularly for claims of subjective nature which depend on a balancing or otherwise discretionary exercise by the competent authority. Considering that users often lack the expertise and resources to engage in a complex mix of factual legal assessments, an oath requirement would likely to generate significant chilling effects.

Intermediaries

One of the potential flaws in IIL regimes lies in the possibilities offered to intermediaries to escape liability even when they are actually favouring infringing activity. For this reason, it is recommendable that regimes conferring broad liability exemptions include a provision, like in section 230 of the Communication Decency Act, which conditions the immunity to the existence of "good faith" in making editorial choices. For example, the existence of such provision led to the non-application of the liability limitation in a case where the intermediary had designed its service (a housing search tool) with a feature (a drop-down menu incorporating racial preferences into the search) that prompted users to infringe the law (specifically, the unfair discrimination law).[115] The requirement of good faith could be interpreted as barring any type of direct financial advantage accruing from the infringing activity, but as noted in the first section above, the specific inclusion of such recognition can result in confusion with the general regime for secondary liability for vicarious infringement, which would still be applicable. As a result, it is preferable not to strictly define via legislation what the meaning of good faith may be in different situations, leaving the courts with the task of determining its application through a contextual analysis. On the other hand, precisely the lack of details on the operation of the "red flag" test in the EU ECD creates problem of inconsistency, and therefore it is preferable the adoption of a uniform solution if a regional instrument is chosen for the protection of intermediaries.

[114]An example is *RIAA v. Verizon*, 351 F.3d 1229 (D.D.C. 2003) where the D.C. Circuit Court of Appeals held that section 512(h) does not apply to content residing on individuals' own computers.

[115]*Fair Housing Council v Roommate.com*, 521 F. 3d 1157 (9th Cir. 2008) (en banc)

But the biggest danger for internet governance from the intermediary reaction to the IIL regime is arguably that of circumvention of the applicable law via contractual arrangements establishing the law with regard to the service offered by that intermediary. This problem is compounded by the fact that the contracts may be structured in such a way that their terms and conditions are opaque or unclear, *de facto* imposed upon the user, and possibly subject to unilateral change. Furthermore, there is a risk that intermediaries do not systematically enforce the terms and conditions of their policies, applying them in a discriminatory fashion. These problems of interaction between law and contracts for the governance of internet communication can be addressed by defining meaningful criteria establishing the limits to the province of contract regulation and, as a consequence, what triggers the liability of the intermediary. This could be done by establishing a set of safe harbours concerning material that is obviously illegal, and can therefore be removed by the intermediary without detailed inquiry and immediate judicial oversight, utilising distinctions such as those between "gross and manifest" and less egregious and apparent violations, or between private law matters (which can be adjudicated by intermediaries, leaving a fully-fledged judicial procedure for potential appeals) and public law matters (where adjudication must conform to higher minimum requirements).[116]

Such norms need not necessarily be developed through a top-down approach. On the contrary, the creation of codes of conduct with multi-stakeholder input should be encouraged in this context. Importantly, these safeguards should include contract law provisions establishing the requirements for a free, express and informed consent. Intermediaries could also be required to specifically notify users about any modification of the terms of services, along with an offer to interrupt the contract and export personal data with no adverse financial consequences.

States

The main concern regarding the state about the adoption of an IIL regime is that such regime be not consistent with the State's duty to protect fundamental rights. This point is related to the safeguards discussed for intermediaries, and could be minimized (as suggested above) through the establishment of mandatory judicial oversight and the definition of criteria (through a framework law or guidelines, such as those for recognition of industry representative bodies in South Africa) establishing the "policy space" for intermediaries in the adoption and implementation of self-regulatory measures. In particular, linking such limits to fundamental rights and principles contained in a Constitution would ensure the supremacy over conflicting rights and interests. In this perspective, a provision such as the "*non-obstante* clause" contained in the Indian Information Technology Act which establishes supremacy over any other conflicting laws would be a powerful instrument to ensure the consistency of the regulatory framework surrounding the IIL regime. In addition, states may utilise their sovereign powers to prevent the disclosure of takedown and personal information requests, so as to escape accountability for extensive censorship or surveillance practices. To avoid this scenario, it is recommended that an IIL regime be built upon the right of access to information and the principle of transparency, applied to the conduct of both intermediaries and governments.

[116]Notwithstanding this preliminary arrangement, the IIL regime should always afford users the opportunity to react with counter-notices and resort to a court for the adjudication of a dispute.

7.Summary and conclusions

The preceding sections have illustrated the wide range of variations in the definition of IIL regimes. While some are more balanced and some more elaborate, it has been shown that flaws exist in all the models addressed throughout the analysis.

The first issue considered has been one of definition of internet intermediary, not only as an abstract concept but also in terms of the specific activities that are insulated from liability through safe harbours. In this context, it has been shown that while countries differ in the number of categories they insulate, the predominant trend is one of distinguishing two types of activities: communication conduits and content hosts. Safe harbours for these categories have different conditions, which are in the former case based on non-interference with the content, and in the latter, on the obligation to act expeditiously upon knowledge of illegal activity.

The second issue analyzed was the scope of liability outside of the safe harbour provisions. In this regard, it was explained that there is a need to clarify explicitly that general principles and doctrines of attribution will continue to apply, and therefore one may well escape liability even failing to qualify for safe harbour. Much of the inconsistency revolves around the concept of knowledge, and the extent to which such knowledge can be inferred. For this reason, it was also recommended that legislators define a clear test on the level of knowledge or awareness of illegality that is sufficient to trigger positive obligations on different kinds of intermediaries.

Subsequently, in reviewing the types of liability limitations that a safe harbour can provide, it was argued that laying out at the outset whether injunctive relief is covered by the safe harbour is extremely important from a legal certainty perspective. This consideration may be very important for small and medium-sized businesses that would be less willing to initiate a court proceeding in light of limited budgetary resources.

The third issue was the modalities of operation of the IIL regime, and was discussed distinguishing:

- Notice and takedown (NTD)
- Notice and notice (NN)
- Notice and disconnection (ND) or graduate response regimes
- Filtering and monitoring.

Several critiques were offered regarding the NTD system, highlighting room for potential improvement. First, it was argued that the regime should establish liability not only for the failure to remove, but also for actual removals in violation of human rights. Second, it was suggested that NTD procedures should specify the need for the claimant to address why the most common defences to infringement actions (such as fair use) would be inapplicable or unsuccessful in the case at issue. The Japanese model was referenced for the good administrative practice by the ISPs to hold a hearing prior to any determination, but criticised for entrusting such delicate decisions to ISPs. At the same time, the effectiveness of diametrically opposed models requiring any determination to be done by a judicial authority was put in doubt. For this reason, in line with the safeguards listed in section 6, the proposal was advanced to define a series of measures which, due to their manifest illegality, could dispense with the more lengthy and costly judicial procedure.

The NN regime was praised for its educational character and its empowerment of users with due process, especially if accompanied by the possibility to issue a counter-notice. Furthermore, it was

stressed that the possibility of a statutory damage sanction in case of failure to comply with the notice and notice requirement is a useful tool, but should provide a significant maximum penalty amount so as to prevent collusion between ISPs and content owners.

The ND or graduate response procedure can also be structured with an educational character, in particular by using the "first strikes," but it was noted the crucial importance that they be accompanied by adequate safeguards of due process, freedom of expression and privacy.

Finally, it was found that a prohibition of imposition of general monitoring obligations for illegal activity is an important element for IIL regimes, but should be complemented by more specific provisions concerning limits to the right holders' ability to obtain an injunction establishing filtering or monitoring obligations to prevent illegal activity. For example, the European experience illustrated that issues to be addressed are the proportionality of such measures and who bears their costs.

In a section devoted to understanding the peculiarities of the African content, it was made clear that any assessment of freedom of expression within the African Charter of Human and Peoples' Rights must follow the formula devised within the International Covenant on Civil and Political Rights by the UN Special Rapporteur on Freedom of Expression Frank La Rue, requiring any measure to be provided by law, serve a legitimate interest and be necessary in a democratic society. At the same time, it was noted that the African charter shows a preference for self-regulatory mechanisms in the media. In this respect, it was cautioned that any such mechanism should include safeguards to avoid the replacement of the public interest with a private order, as stressed also in the Joint Declaration on Freedom of Expression and the Internet. The same declaration also highlighted the importance of the principle of transparency, applied both in the context of an ISP's traffic management practices and to any filtering measures. This principle is in line with the right of access to information, which the Draft Model Law for AU Member States on Access to Information endeavoured to implement.

With regard to the right to privacy, it was noted that although it is not recognised in the African charter as such, it is increasingly part of local laws and constitutions. Moreover, the right to privacy is inextricably linked to the realisation of freedom of expression, as pointed out by the UN Special Rapporteur on Freedom of Expression (most recently in its 2013 annual report[117]).

Finally, the concept of due process was addressed by noting that the African charter includes an even wider protection of the presumption of innocence than other human rights instruments, since it applies to non-criminal proceedings as well. Accordingly, any framework for IIL must not set the burden of proof irreversibly in favour of the claimants. Furthermore, it was stressed that, in accordance with the human rights framework of the charter, any mechanism devised for the liability of intermediaries in Africa must respect the right of access to an independent and impartial tribunal and the right to appeal.

The last section outlined a series of threats to the proper functioning of an IIL regime, and proposed a number of safeguards that can be devised to address those concerns.

To prevent strategic use of IIL regimes by users and complainants, an IIL regime could include an abusive litigation sanction, and in the case of complainants, a requirement to consider the validity of common defences before submitting the infringement complaint. In general, judicial oversight

[117] F. La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedomof opinion and expression*, (A/HRC/23/40), para. 24-26

would be necessary to ensure the competence, independence and impartiality of the assessment of legality.

As to the conduct of intermediaries, introducing the requirement of good faith would prevent fraudulent reliance on the safe harbour in cases where the intermediary is encouraging or profiting from the infringing activity. It was also stressed that a general framework could be devised to identify those norms that cannot be overridden by contractual regimes agreed upon between the intermediaries and their users. For example for distinguishing between "gross and manifest" violations of the law which can be adjudicated by intermediaries without following a fully-fledged judicial procedure, and less clear determinations where adjudication must conform to standard judicial requirements. The line between these two sets of cases could be drawn by codes of conduct developed by industry associations, encouraging multi-stakeholder participation. However, even accelerated procedure must comply with minimum standards of due process- namely the possibility to obtain full judicial review before an independent and impartial tribunal.

Finally, turning to possible abuses by the states, two types of safeguards were suggested to prevent their non-implementation of the rights and principles enshrined in the IIL regime. First, as discussed also in the safeguards for intermediaries, the existence of a robust system of appeal to a judicial authority. Second, a clear system for the definition of the limits to the power of intermediaries to self-regulate, linking those limits to the fundamental rights and principles contained in state constitutions. This would ensure that states do not turn a blind eye on problematic codes of conduct, thus acting consistently with their positive obligation to protect human rights. Furthermore, a general suggestion was given to design the IIL regime around the right of access to information and the principle of transparency, in order to ensure at the same time accountability by governments and intermediaries themselves.