SPACES AND RESPONSIBILITIES: A REVIEW OF FOREIGN LAWS AND AN ANALYSIS OF PHILIPPINE LAWS ON INTERMEDIARY LIABILITY*

NOTE

*Gemmo B. Fernandez***
*Raphael Lorenzo A. Pangalangan****

ABSTRACT

While the Internet facilitates a diverse assortment of methods of communication, it as well poses a risk of harm to the exercise and enjoyment of human rights and freedoms. As a response to this, authorities have implemented measures without directly targeting the origin nor the recipient of Internet communications by imposing liability on the Internet intermediaries in charge of the communication process itself. The paper forwards the vertical approach to be appropriate in dealing with the liability of Internet intermediaries as it applies different regimes depending on the area of substantive law infringed. With regard to specific regimes, it submits that the most reasonable regime is that of safe harbour as it tends to balance the responsibilities of intermediaries and the burden that it has to discharge. The paper suggests that the Philippines has impliedly accepted the safe harbour regime based on it imposition of liability on the intermediary. However, while laws dealing with copyright, child pornography, and cybercrime have been promulgated, they do not seem to address other areas of regulation which other jurisdictions have addressed. Finally, it notes that Philippine intermediary laws fail to distinguish between the nature of different intermediaries, or worse, fail to address the liability of other types of intermediaries.

---

* *Cite as* Gemmo Fernandez & Raphael Lorenzo Pangalangan, *Spaces and Responsibilities: A Review of Foreign Laws and an Analysis of Philippine Laws on Intermediary Liability*, 89 PHIL. L.J. 761, [page cited] (2015).

** J.D., University of the Philippines (2016, expected). B.S. Applied Mathematics in Finance, Ateneo de Manila University (2011); First Place, Monroe E. Price Media Law Moot Court Competition on Freedom of Expression, University of Oxford Programme for Comparative Media Law and Policy, International Rounds (Oxford University, 2015).

*** J.D., University of the Philippines (2016, expected). B.A. Philosophy *cum laude*, University of the Philippines (2012); First Place, Monroe E. Price Media Law Moot Court Competition on Freedom of Expression, University of Oxford Programme for Comparative Media Law and Policy, International Rounds (Oxford University, 2015).

1. INTRODUCTION

The nature of the Internet may be considered simply as a series of inter-connected networks, consisting of privately owned servers, routers, and backbones that communicate using a suite of common languages. [1] Notwithstanding this seemingly plain characterisation, the Internet has fundamentally altered the capacity of individuals to communicate with one another resulting to both positive and negative changes.[2] The rise of the Internet has led to accessible and efficient forms of communication from forums, media-hosting services, blogs, and social media. It has also increased the efficiency of dealings between firms and changed the ways consumers and commercial establishments enter into transactions.[3] This amplification in the capacity of individuals to communicate or transact with one another, however, has been recognised to be prone to abuse and has been used to violate laws.[4] Hence, while the Internet facilitates a diverse assortment of methods of communication, it poses a risk of harm to the exercise and enjoyment of human rights and freedoms.[5] This problem is further exacerbated by two factors: first, a lack of central authority that determines what content can be hosted online or who can access said network;[6] second, there arises difficulty in regulation, as the Internet is a global forum where the limitations of national territory are of little relevance.[7]

In fact, even the extent and nature of regulation content on the Internet is subject to debate. Though it is well established that the right to freedom of expression encompasses Internet-based modes of expression,[8]

---

[1] David Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under § 230 of the Communications Decency Act* (2010), 43 LOY. L.A. L. REV. 373, 383 *citing* Jay Kesan and Rajiv Shah, *Fool Us Once Shame on You-Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System* 79 WASH. U. L.Q. 89, 131-32 (2001); Dawn Nunziato, *The Death of the Public Forum in* Cyberspace (2005) 20 BERKELEY TECH. L.J. 1115, 1116 (2006).

[2] *Id. citing* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM, 32 (2006).

[3] Ronald Mann & Seth Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 244 (2005-06).

[4] *Id.* at 245.

[5] Editorial Board of Pravoye Delo and Shtekel v. Ukraine, (ECtHR, May 5, 2011).

[6] Ardia, *supra* note 1, at 384 *citing* INTERNET ARCHITECTURE BOARD, ARCHITECTURAL PRINCIPLES OF THE INTERNET (Brian Carpenter ed. 1996) 2-4.

[7] Benoît Frydman & Isabelle Rorive, *Regulating Internet Content through Intermediaries in Europe and the USA*, 23 ZEITSCHRIFT FÜR RECHTSSOZIOLOGIE 41, 44 (2009) *citing* Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

[8] General Comment 34 in Article 19 (Freedom of Opinion and Expression), U.N. Doc. CCPR/C/GC/34 (2011).

there is a dearth of tangible criterion as to where the fine line between fair use and abuse is drawn. This conflict is illustrated by the fact that courts from various jurisdictions have ruled just as variedly as to how the Internet is to be treated. While some authorities have ruled that the Internet is entitled to the same amount of protection as traditional media,[9] others have decided in the opposite, finding that the harm posed by content on the Internet is certainly higher than that of traditional media which thereby necessitates appropriate adjustments in regulation.[10]

Recently, state actors have begun to implement measures without directly targeting the origin nor the recipient of Internet communications.[11] Due to the fact that the imposition of liability on the content provider or the recipient is not always possible or efficient, what became a more successful strategy is to put pressure on the Internet intermediaries in charge of the communication process itself.[12] In the past two decades alone, numerous states have enacted laws regulating the Internet by imposing liability on the intermediary.

In 1996 and 1998, the US enacted two statutes that touched upon intermediary liability. The first is the Communications Decency Act of 1996 ("CDA") that regulated indecent materials on the Internet. While a number of its provisions have been struck down in the case of *Reno v. ACLU*,[13] Section 230 of the act that protects Internet services providers ("ISPs") from liability for restricting access to certain material or giving others the technical means to restrict access to that material remains in force. On the other hand, the Digital Millennium Copyright Act[14] ("DMCA") criminalised the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works while providing some exemptions from direct and indirect liability of intermediaries. In 2000, the European Union adopted the Electronic Commerce Directive [15] ("EC Directive") that harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of

---

[9] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

[10] Editorial Board of Pravoye Delo and Shtekel v. Ukraine, (ECtHR, May 5, 2011).

[11] Seth Kreimer, *Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 12, 14 (2006).

[12] Frydman & Rorive, *supra* note 7, at 44.

[13] 521 U.S. 844 (1997).

[14] 17 U.S.C. §§ 512, 1201–1205, 1301–1332; 28 U.S.C. § 4001.

[15] Council Directive (EC) 2000/31 concerning certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L178 (2000).

intermediary service providers. Other states have since enacted laws dealing with the liability of intermediaries.[16]

Recognizing the need to provide safeguards in the Internet, the Philippines has likewise enacted laws that impose liabilities on ISPs. It is submitted, however, that these legislations are not without fault. This paper aims to critique Philippine laws on intermediary liability in light of existing laws and practices in other jurisdictions. Part II discusses the nature of Internet intermediaries and categorises these into four: mere conduits, information locators, caching providers, and hosts. Part III examines the regimes or models of liability: strict, safe harbour, and general immunity. Part IV discusses the areas of regulation of intermediaries: copyright infringement, defamation, and illegal or harmful content. Finally, Part V analyses Philippine laws that deal with intermediaries: Rep. Act No. 8792 ("Electronic Commerce Act of 2000"), Rep. Act No. 9775 ("Anti-Child Pornography Act of 2009"), Rep. Act No. 10175 ("Cybercrime Prevention Act of 2012"), Senate Bill No. 53 (Magna Carta for Philippine Internet Freedom), and Senate Bill No. 1091 (Magna Carta for Philippine Internet Freedom of 2013).

2. NATURE OF INTERMEDIARIES

Before delving into an analysis of Internet intermediary laws, it is helpful to define the terms that will be discussed, beginning with the very subject of this paper—the intermediary.

The EC Directive broadly defines Internet intermediaries as information service providers engaged in "information society services," namely "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[17] The Directive provides that "information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them."[18] By this definition, these services

---

[16] These states include, but are not limited to: Kenya, Nigeria, Rwanda, South Africa, Tanzania, Australia, China, India, Malaysia, Singapore, South Korea, Taiwan, Belgium, Czech Republic, Finland, Georgia, Germany, Greece, Ireland, Italy, Netherlands, Poland, Portugal, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Canada, Mexico, U.S.A., Azerbaijan, Iran, Israel, Jordan, Turkey, Argentina, The Bahamas, Bolivia, Brazil, Chile, Colombia, Guatemala, Venezuela. Regional organisations that have enacted similar measures include: African Union, European Union, and the Caribbean Community.

[17] Council Directive (EC) 2000/31, *supra* note 15, art. 2(a) referring to Council Directive 98/34, art. 1(2) as amended by Council Directive 98/48.

[18] *Id.* at 17.

include "the offering of on-line information or commercial communications, or the providing of tools allowing for search, access and retrieval of data, [...] transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service."[19] While radio and television broadcasts are excluded, those "services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are [considered] information society services."[20]

Furthermore, the EC Directive defines a "service provider" as "any natural or legal person providing an information society service."[21] On the other hand, an "established service provider" is a "service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider."[22]

The foregoing definition is expansive, to the effect that it covers a variety of activities made in the Internet; and it is also ambiguous. At present, an intermediary may provide services ranging from transmitting signals across networks to allowing users to store information on the Internet. Hence, it seems that the treatment of intermediaries must take into consideration the nature of its activity. Proceeding from this, it appears to be more helpful to examine the nature of an intermediary based on the activity it undertakes.[23] Under this analysis, intermediaries could fall under four categories: mere conduit, information locators, caching providers, and host service providers.[24]

---

[19] *Id.*

[20] *Id.*

[21] *Id.* at art. 2(b).

[22] *Id.* at art. 2(c).

[23] Pablo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA HIGH TECH L.J. 111, 119 (2002).

[24] Jonina Larusdottir, *Liability of Intermediaries for Copyright Infringement in the Case of Hosting on the Internet*, 47 SC.ST.L. 471, 473 (2004); The same categories are provided in: South Korea's Copyright Act (last amended by Act No. 12137, Dec. 30, 2013), South Africa's Electronic Communications and Transactions Act (Act N. 25/2002, July 31, 2002), Poland's Act of July 18, 2002 on Providing Services by Electronic Means (O.J. 2002 No. 144, item 1204 as amended), Portugal's Decree-Law No. 7/2004 (Jan. 7, 2004), Slovenia's Electronic Commerce Market Act (May 30, 2006).

2.1. Mere Conduits

As to the first category, a "mere conduit" may be considered a "network-operator" that provides the facilities, such as cables and routers, for the dissemination of the material, or "access provider" that provides access to the Internet.[25] The activities engaged in by a mere conduit could therefore fall under two distinct acts. The first includes "the transmission in a communication network of information provided by a recipient of the service."[26] Here, the intermediary serves a passive role by acting as a mere "carrier" of data that is provided by third parties through its network. The second is the act of "providing Internet access."[27] In general, the sole purpose of mere conduits is transmitting information in the network. Information, while they may be automatically stored, is not kept for any period longer than that is reasonably necessary for the transmission.[28]

In comparison with other categories of intermediaries, mere conduits possess the least liability. Under the EC Directive, "the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission."[29] These have been incorporated in EU member states' laws.[30]

Furthermore, the regime set up by article 19 of the EC Directive is similar to that enforced under the DMCA.[31] In the case of *Record Industry Association (RIAA) v. Verizon*,[32] RIAA sought to compel Verizon, an Internet service provider, to identify subscribers whom it believed had infringed their members' copyrights. The District Court granted the motion to compel production. The Court of Appeals reversed and ruled that Verizon was acting as a conduit for file sharing and, therefore, did not involve the storage of infringing material on its servers.[33]

---

[25] *Id.*

[26] Baistrocchi, *supra* note 23, *citing* Council Directive (EC) 2000/31, *supra* note 15, art. 12(1).

[27] *Id.*

[28] *Id.*; UK Dep't of Trade and Industry, *Electronic Commerce Directive* (2002), Ch. 6.

[29] Council Directive (EC) 2000/31, *supra* note 15, at art. 12(1).

[30] *See* Czech Republic's Law No. 480/2004 (July 29, 2004); Ireland's S.I. No. 68 of 2003; Italy's Legislative Decree N. 70 (Apr. 9, 2003); Poland's Act of July 18, 2002 on Providing Services by Electronic Means (O.J. 2002 No. 144, item 1204 as amended); Portugal's Decree-Law No. 7/2004; Slovenia's Electronic Commerce Market Act (May 30, 2006).

[31] Frydman & Rorive, *supra* note 7, 53.

[32] 351 F.3d 1229 (D.C. Cir. 2003).

[33] *Id.*

2.2. Information Locators

The second category of intermediaries is that of "information locators." Often referred to as "search engines," these intermediaries make tools available to users for finding websites where the information they seek is located.[34] As such, these intermediaries may be considered as "one of the most important actors in the everyday development of the Internet."[35] An information locator may perform its activities by creating databases of websites arranged by thematic, geographic, or some other criteria that facilitate users in finding the sought-after data.[36]

Under the DMCA, information locators are not liable for linking users to websites containing illegal materials so long as the information locator: (a) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (b) 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 (c) upon notification of claimed infringement, responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[37]

This liability for linking seems to have been excluded in the EC Directive. Since article 14 of the Directive requires storage, this may imply that the act of hyperlinking to illegal content does not fall within the purview of storage and, as a result, liability may not attach.[38]

Furthermore, other factors may be taken into consideration in determining whether the information locator is liable for linking to illegal material. In *Bleyer v. Google Inc.*,[39] the Australian Supreme Court held that Google is not a publisher of its search results, having no human input in the production of search results, save for the creation of its search algorithm. This ruling is in line with that of *Rana v. Google Australia Pty. Ltd.*[40] where the Australian Federal Court held that Google Australia had no control over the search results that included defamatory words and was therefore free from

---

[34] Larusdottir, *supra* note 24.

[35] Baistrocchi, *supra* note 23, *citing* ACLU v. Reno 929 F. Supp. 824, 837 (E.D. Pa. 1996).

[36] *Id.*

[37] 17 U.S.C. § 512(c).

[38] Charlotte Waelde & Lilian Edwards, Online Intermediaries and Copyright Liability (Apr. 2005) (World Intellectual Property Organization Workshop Keynote Paper, Geneva).

[39] [2014] NSWSC 897, Aug. 12, 2014.

[40] [2013] FCA 60, Feb. 7, 2013.

liability. In its decision in March 2010,[41] the South Korean Supreme Court ruled that *Yahoo* cannot be held liable for merely allowing users search copyright infringing materials to be searched on their portals. On the other hand, in *Coolstreaming and Calciolibero*,[42] the Italian Supreme Court distinguished the actions of the intermediaries therein from common search engines as the latter merely provides the users with online guidance without which the infringement would not be possible while the former provided online guidance that made the illegal act possible.

2.3. Caching Service Providers

The third category of intermediaries is that of caching service providers. Intermediaries perform the act of caching to avoid saturating the Internet with repetitive demand of a particular material by storing copies of this material on local servers. As a result, information is delivered to users more efficiently as the information travels less distance between the storage to the user. Here, the action of the intermediary is often automatic, intermediate and temporary.[43]

Under the EC Directive, an intermediary performing caching service is not liable for the providing access to the material stored when it is in "no way involved with the information transmitted." Hence, the intermediary is immune when it "does not modify the information that the user transmits." However, "this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information."[44] Other states have followed the same condition for imposing liability on caching.[45]

2.4. Host Service Providers

The last category pertains to host service providers. In general, host service providers offer space on their servers where users may store their

---

[41] Supreme Court of South Korea, Decision 2009Da4343 (Mar. 11, 2010).

[42] 33945/06 (Oct. 10, 2006).

[43] Baistrocchi, *supra* note 23, at 120.

[44] EC Directive, *supra* note 15, recital 43 *cf.* art. 13.

[45] These state legislations include, but are not limited to: Taiwan's Copyright Act (as amended on Jan. 22, 2014); Rwanda's Law No. 18/2010 (relating to Electronic Messages, Electronic Signatures and Electronic Transactions, Mar. 12, 2010); South Africa's Guidelines No. 29474/2006 (Dec. 14, 2006); Czech Republic's Law No. 480/2004 (July 29, 2004); Ireland's S.I. No. 68 of 2003; Italy's Legislative Decree N. 70 (Apr. 9, 2003); Slovakia's Law No. 22/2004 (Dec. 3, 2003); Slovenia's Electronic Communications Act (Dec. 20, 2012); Canada's Copyright Modernization Act (SC 2012).

content.[46] In said space, intermediaries may allow users to post materials either at a cost or for free.[47]

Under the EC Directive, immunity is granted to host service providers so long as: "(a) the provider does not have actual knowledge of unlawful activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[48] In both conditions, "the recipient of the service is acting under the authority or the control of the provider."[49] Lastly, "upon obtaining actual knowledge or awareness of illegal activities, [the provider] has to act expeditiously to remove or to disable access to the information concerned" provided that "the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level."[50]

It can be gleaned from the foregoing that mere knowledge of illegal or infringing activity is not enough to hold an intermediary liable, provided that it expeditiously removes the illegal or otherwise unlawful content or disables access to it. Moreover, while the Directive takes "into account all matters in the particular circumstances to be relevant,"[51] such as notice, it fails to provide for a particular method on how the intermediary is to be informed of the alleged infringement.[52] The Directive as well omits to establish a standard to determine when the intermediary, despite the absence of notice, is "aware of facts or circumstances from which the illegal activity or information is apparent."[53] This must be contrasted with the DMCA which provides for such mechanisms. Further, the term "actual knowledge or awareness" is left undefined in the EC Directive. This would be discussed in a latter part of this paper.

---

[46] Larusdottir, *supra* note 24.

[47] Baistrocchi, *supra* note 23, at 116 *citing* Rosa Julia-Barcelo, *Liability for Online Intermediaries: A European Perspective*, 10 CENTRE DE RECHERCHES INFORMATIQUE ET DROIT 7 (1998).

[48] Council Directive (EC) 2000/31, *supra* note 15, art. 14(1).

[49] *Id.* at art. 14(2).

[50] *Id.* at recital 46.

[51] Council Directive (EC) 2000/31, *supra* note 15, art. 22.

[52] Baistrocchi, *supra* note 23, at 124.

[53] Council Directive (EC) 2000/31, *supra* note 15, art. 14(2).

The same requirements are required in other states' legislations.[54] Other jurisdictions, however, have set-forth additional requirements for intermediaries to escape liability. The DMCA, in dealing with copyright infringements, further provides that in order for the intermediary to avail of the immunity, it must "not receive a financial benefit directly attributable to the infringing activity."[55] In Australia, host service providers must include a reasonably implemented termination policy for repeat infringers and a notice and takedown regime.[56] South Korea's Copyright Act imposes additional requirements for peer-to-peer file sharing service providers to implement filtering mechanisms.[57]

3. REGIMES OF LIABILITY

Preliminarily, there are two general approaches to the liability of intermediaries: horizontal and vertical. In the horizontal approach, a liability regime is applied to any infringement of the law imposing intermediary liability.[58] The EC Directive follows this approach. Thus, whether the liability arises due to defamatory content or infringement of copyright, the same regime is applied.[59] On the other hand, the vertical approach applies different regimes depending on the area of substantive law infringed. This is the approach adopted by the United States. The DMCA is applied when dealing with issues copyright infringement while the Telecommunications Act of 1996[60] deals with liability derived from violations of other laws.[61]

---

[54] These legislations include, but are not limited to: Hong Kong's Information Technology Act 2000 (as amended by the Information Technology Act 2008); Malaysia's Communications and Multimedia Content Code (Sept. 1, 2004); Singapore's Copyright Act (Parliamentary Legislation, Chapter 63, Revised Edition 2006, Jan. 31, 2006); Rwanda's Law No. 18/2010 (relating to Electronic Messages, Electronic Signatures and Electronic Transactions, Mar. 12, 2010); South Africa's Electronic Communications and Transactions Act (Act N. 25/2002, July 31, 2002); Chile's Law No. 20.435 (May 4, 2010); Portugal's Decree-Law No. 7/2004 (Jan. 7, 2014); Russia's Federal Law No. 364-FZ (amending Legislative Acts of the Russian Federation Concerning the Protection of Intellectual Rights in Information and Telecommunications Networks, Nov. 24, 2014).

[55] 17 U.S.C. § 512(c) (2002).

[56] Copyright Legislation Amendment Act of 2004, § 116AH(1).

[57] Copyright Act (amended by Act No. 12137, Dec. 30, 2013), § 104.

[58] Baistrocchi, *supra* note 23, at 117 *citing* Rosa Julia-Barcelo, *On-line Intermediary Liability Issues: Comparing EU and US Legal Frameworks*, 22 EUR. INTELL. PROP. REV. 105, 108 (2000).

[59] Larusdottir, *supra* note 24, at 482; Baistrocchi, *supra* note 24, at 117.

[60] Telecommunications Act of 1996, Pub. L. 104-104, Title V, 110 Stat. 56, 133-43 (1996).

[61] Baistrocchi, *supra* note 23, 117.

Some authors argue that a horizontal approach is favourable because intermediaries do not have to monitor the content of the material published by their customers.[62] The reason for this is that adopting a vertical approach would impose a disproportionate burden on intermediaries as they have to examine all content that are stored in their spaces, regardless of the nature of the activity. Further, this entails the possibility of converting intermediaries into censorship agents.[63]

On the other hand, it is submitted that the vertical approach is more fitting. First, as will be discussed in the latter part of this paper, different areas of regulation call for different application of intermediary liability laws. For instance, laws that deal with illegal or harmful content, such as child pornography, require more responsibility on the part of the intermediary as compared to laws that deal with copyright infringement. Requiring a blanket application of the regulation would in effect afford less protection to users. Second, the possibility of turning intermediaries into censorship agents is hinged on the specific regime applied. In the application of safe harbour regime, a proper method of notice and takedown coupled with the clause in the restoration of content counter-balances the fears of over-censorship or chilling effects.[64]

International regimes to regulating intermediaries can be properly classified into three categories: strict liability, safe harbour, and total immunity.[65] These regimes will be discussed in seriatim.

3.1. Strict Liability

Under the "strict liability regime," intermediaries are liable in the same way as content providers are for illegal or infringing material.[66] This is considered to be the most restrictive regime as it holds the intermediary liable without considering its knowledge and extent of control over the content disseminated through its network.[67] As a result, it entails a heavy burden on the part of the intermediary to monitor its network to ensure that no illegal content is disseminated.

---

[62] *Id.*

[63] *Id.*

[64] Frydman & Rorive, *supra* note 7, at 53.

[65] Waelde & Lilian Edwards, *supra* note 38, at 22.

[66] *Id.* at 19.

[67] Baistrocchi, *supra* note 23, at 117 *citing* Julia-Barcelo, *supra* note 47, at 10.

In support of this regime, it is put forward that intermediaries are in a better position than the copyright-holders to prevent or to stop the infringing activity as they can block access to infringing material.[68] While software is available that can facilitate monitoring,[69] the operation of such a program would nonetheless require human monitoring services to screen the material hosted in the network that incessantly changes dramatically over a short period of time. This makes its operation almost impossible.[70] Nevertheless, with the advent of modern software, it has been observed that such may be done. In a French High Court case, Yahoo was found to have the capacity block access to its Nazi memorabilia auction pages to all persons from France.[71]

The regime is commonly applied in states where intermediaries have been used to disseminate subversive, seditious, and politically unsettling material. In such scenarios, the intermediaries are encouraged forcibly to act as an arm of state censorship.[72] In China, strict liability is imposed on intermediaries to refrain from "producing, posting or disseminating pernicious information that may jeopardise state security, disrupt social stability, contravene laws and regulations, and spread superstition and obscenity."[73] In the other jurisdictions however, such measure is seen to impede on the freedom of speech by creating a chilling effect.[74] For instance, in a 2013 decision of the Italian Court of Appeals, it was decided that the strict liability is not compatible with freedom of expression and rejected the appeal to impose the same.[75]

3.2. Safe Harbour

The second regime is that of "safe harbour." Under this regime, intermediaries are only held liable for infringement if they had knowledge that the infringing material was hosted on their facilities.[76] Furthermore, safe

---

[68] Erik Hagen, *On-line Service Provider Liability: The Latest US Copyright Conundrum*, 7 ENT. L.R. 274, 279 (1996).

[69] Carter Kirkwood, *When Should Computer Owners be liable for copyright Infringement by Users?* 69 U. CHI. L. REV. 709, 730 (1997).

[70] Larusdottir, *supra* note 24, at 475, *citing* Julia-Barcelo, *supra* note 47.

[71] Waelde & Edwards, *supra* note 38, at 20, *citing* LICRA et UEJF v. Yahoo! Inc. and Yahoo France, Tribunal de Grande Instance de Paris, 20/11/2000.

[72] *Id.* at 19, *citing* Chris Reed, *Liability of Online Information Providers – Towards a Global Solution* 17 INT'L. REV. L. COMPUTER & TECH. 255 (2003).

[73] *Id.*; Baistrocchi, *supra* note 23, at 114.

[74] *Id.*; Frydman & Rorive, *supra* note 7, at 56.

[75] María Belén c/ Google Inc. y Otro s/ Daños y Perjuicios, Expte.AR/JUR/21886/2013, May 13, 2013.

[76] Larusdottir, *supra* note 24, at 476; Note that other states have also adopted the safe harbour regime: Australia's Copyright Legislation Amendment Act 2004; India's Information Technology Act; Malaysia's Copyright Amendments Act of 1990 and 2012; Singapore's

harbour laws often include a "notice and takedown mechanism." Under this provision, upon receiving knowledge that a particular content is illegal or that it infringes on an individual's rights, the intermediary must remove the material or disable access to it. The DMCA, in dealing with copyright infringements, requires hosts to designate an agent that would "receive notifications of claimed infringement." Further, the hosts must provide the agent's details to the public through the Copyright Office.[77] This mechanism relating to agents is absent in the EC Directive.

There are two approaches as to what constitutes knowledge: actual and constructive.[78] Under "actual knowledge," the intermediary is held liable if it intentionally violates the law or infringes on an individual's rights.[79] On the other hand, under "constructive knowledge," the law may make the determination if the intermediary, under certain factors, should have reasonably presumed that a material is illegal or infringing on an individual's rights.[80]

Some authors argue that the latter approach should be adopted. According to them, "[i]mposing the actual knowledge standard would lead to a low risk of liability for the [intermediaries], as in that case it must be established that the [intermediary] actually knew about the infringing material in order to trigger the potential liability."[81] As a result, it provides that intermediary an incentive to not monitor the content hosted in its facilities. Applying the constructive knowledge approach negates this possibility since the standard imposes a higher risk of liability for intermediaries, and thus forces them to enact mechanisms to avoid liability.[82]

It can be counter-argued, however, that the effectiveness of the measure depends on law's notice and takedown mechanism. If the provisions are properly drafted, the fact that an infringing material is stored in the facilities of the intermediary may be brought to its attention without imposing on it a heavier burden than that of constructive knowledge.

On the other hand, the application of constructive knowledge approach begs two problems. The first problem lies on the determination of

---

Copyright Act; South Korea's Copyright Act; and other members of the European Union that have adopted the EC Directive as part of their respective legislations.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] Baistrocchi, *supra* note 23, at 114.

[81] Larusdottir, *supra* note 24, at 477.

[82] *Id.*

whether the intermediary had knowledge of the circumstances surrounding the illegal content.[83] The second problem is that of judging if the illegality of the material is apparent.[84]

In some jurisdictions, other factors are taken into consideration. In an Australian Federal Court decision,[85] the extent of control of the intermediary was considered. In that case, a news website was found to be liable for the comments of its readers because it had knowledge of these comments and had actually sought these from its readers and reserved the right to modify or not to publish such. In a South Korean Supreme Court decision,[86] it was held that a comprehensive analysis of the following factors should point to responsibility on the part of intermediary: (a) the posting's purpose, content, duration and method; (b) the damages it has caused; (c) the relationship between the speaker and the injury-claimant; (d) the claimant's attitude including whether rebuttal or takedown was requested; (e) the size and nature of the site posted, (f) the degree of for-profit nature of the site; (g) when the operator knew or could have known the posting's content; and (h) the technological and pecuniary difficulty in taking down, etc. Having said so, the Supreme Court reversed the lower court that imposed the liability for pre-takedown exposure.

Significantly, in the case of *RMB v. Google*,[87] the Argentinian court ruled that in the case of ostensible infringing content, a private notification as to the illegality of the content hosted, from any person, not necessarily the affected party, would suffice. Ostensibly infringing conduct constitutes "child pornography, data that might be useful to commit a crime, that might endanger people's lives, that promotes genocide, racism or any other discriminatory or violent action, that might trump crime investigations, that are a serious offence to honour, obviously faked pictures, or any serious invasion to privacy, publishing images that because of its nature are intended to be private, even if not sexual."[88]

Finally, one key feature of the DMCA is that of the "put back" procedure. This may be considered to obtain more complete protection for all the actors involved namely: the intermediary, the content owner, and the user possibly harmed. Through this procedure, a content owner may request

---

[83] *Id.* at 484.

[84] *Id.*

[85] Clarke v. Nationwide News Pty. Ltd. (t/as The Sunday Times) (2012) 289 ALR 345; [2012] FCA 307 (Mar. 27, 2012).

[86] Supreme Court of South Korea Decision 2002Da72194 (June 27, 2003).

[87] R. *M. B. c/ Google Inc.*, Dec. 5, 2014, MJ-DOC-6993-AR.

[88] *Id.*

that the content removed be replaced or access be re-enabled by the intermediary upon proof that the content does not infringe on the rights of others or is not otherwise illegal. Moreover, it shields that intermediary from liability if it can claim "good faith [in] 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, regardless of whether the material or activity is ultimately determined to be infringing."[89]

3.3. General Immunity

The third regime is that of "general immunity." Under this regime, "intermediaries left to their own devices will, for commercial reasons, naturally take on an editorial and filtering role, so long as they are given protection from the risk entailed in being seen as publishers, distributors or the like."[90] The Communications Decency Act of 1996 ("CDA") follows this regime. Section 230(c) of the CDA, also referred to as the "Good Samaritan Clause,"[91] provides in part: "No provider or user of an interactive computer service shall be treated as publisher or speaker of any information provided by another content provider."[92] It is further stated that no provider or user shall be held liable on account of any action voluntarily taken in good faith in the "blocking and screening of offensive material."[93]

The problem with this regime is that since intermediaries are totally immune from liability, the reasonable demands for take down can be ignored without the threat of litigation.[94] For instance, in the case of *Zeran*, the individual suing for defamation by an anonymous user was left without recourse as the intermediary was held to be immune from liability.[95] In the case of *Blumenthal v. Drudge*,[96] the intermediary was also exculpated as the individual who posted the defamatory content was a third-party notwithstanding the fact that the intermediary benefited from the posting of the material. [97] Nevertheless, modern trends have challenged the holding based on general immunity as seen in the cases of *Barrett v. Rosenthal* and *Grace v. eBay, Inc.*[98].

---

[89] 17 U.S.C. § 512(h).

[90] Waelde & Edwards, *supra* note 38, at 20.

[91] 47 U.S.C. § 230(c).

[91] § 230.

[93] Jane Doe No. 14 v. Internet Brands, Inc., No. 12-56638 (9th Cir. Sept. 17, 2014).

[94] Waelde & Edwards, *supra* note 38, at 21.

[95] *Id. citing* 1997 U.S. Dist. Lexis 3429 (EDVA Mar. 21, 1997).

[96] Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

[97] Waelde & Edwards, *supra* note 38, at 21, *citing* 1998 BNA EC&L 561.

[98] *Id. citing* Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 9 Cal. Rptr. 3d 142 (Cal. App. 1st Dist. 2004); Grace v. eBay, Inc., 120 Cal. App. 4th 984 (Cal. App. Ct. 2004).

In the case of *Jane Doe No. 14 v. Internet Brands*,[99] the limitations of the general immunity of Section 230(c) of the CDA were further defined. There, it was ruled that the CDA does not bar Jane Doe's failure to warn claim as it did not seek to hold Internet brands liable as the "publisher or speaker" of any information provided by another user. It was further stated that liability would not discourage the intermediary from filtering of third party content." The core policy of Section 230(c) is to provide protection for intermediary in blocking and screening of offensive material. This means that "a website should be able to act as a 'Good Samaritan' to self-regulate offensive third party content without fear of liability."

4. AREAS OF REGULATION

Having discussed the nature of intermediaries and the regimes of liability, its application in different areas of substantive law is now examined. As previously submitted in Part III, the vertical approach in dealing with intermediary liability is more apt than that of the horizontal approach as it takes into consideration the peculiar nuances in the different areas of substantive law, namely: copyright, defamation, illegal or harmful content, and deceptive or misleading conduct.

4.1. Copyright

The efficiency of online connection has enabled copyrighted material to be easily duplicated and disseminated to Internet users. Consequently, as the Internet advances, more materials are distributed to the substantial injury of copyright holders due to infringement.[100] While copyright laws generally hold the content-provider liable for any infringement,[101] the extent of liability for intermediaries is less clear. Clearly, when intermediary and the content-provider are one and the same or when the content-provider is acting under the control and supervision of the intermediary, the latter may be held primarily liable.[102] In the absence of control and supervision, however, the liability of the intermediary depends on the nature of the intermediary and the regime adopted by the regulating state.

The DMCA and EC Directive adopted the safe harbour regime in dealing with the liability of intermediaries as to copyright infringement. In both jurisdictions, the liability depends first on the nature of the intermediary.

---

[99] No. 12-56638 (9th Cir. Sept. 17, 2014).

[100] Larusdottir, *supra* note 24, at 472.

[101] *Id.*

[102] Waelde & Edwards, *supra* note 38.

In the DMCA, intermediaries are classified either as transmission service provider, caching service provider, hosts, and information locator provider.[103] The EC Directive categorises intermediaries as: mere conduits, caching service providers, and hosts.[104]

For mere conduits, both of the aforementioned laws exempt the intermediary if it: "(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission."[105] The DMCA, however, further requires that: "(a) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (b) the material is transmitted through the system or network without modification of its content."[106]

As to caching service providers, the DMCA and EC Directive allows for immunity if the intermediary: (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[107]

Under the DMCA, search engines are immune from liability if it: "(a) does not have actual knowledge that the material or activity is infringing; (b) not aware of facts or circumstances from which infringing activity is apparent; and (c) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material." Lastly, the search engine must "not receive a financial benefit directly attributable to the infringing activity, in a

---

[103] 17 U.S.C. § 512.
[104] EC Directive, *supra* note 15, art. 12-4.
[105] *Id.* at art. 12.
[106] 17 U.S.C. § 512(a).
[107] EC Directive, *supra* note 15, art. 12.

case in which the service provider has the right and ability to control such activity."[108]

Lastly, for host service providers, both the DMCA and the EC Directive exempt the intermediary from liability if it: (a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; and (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[109]

Other states have also followed the same model as that of the DMCA. Notably, many of these legislations were passed due to the existence of free trade agreements with the US. Australia's Copyright Legislation Amendment Act of 2004, amending the Trade Agreement Implementation Act of 2004, provides intermediaries safe harbour provided that there exists reasonably implemented termination policy for repeat infringers and a notice and takedown regime.[110] As an application, in a decision of the lower court, an intermediary was found liable in relation to copyright infringement as it could have chosen not to accept or to remove links to infringing content. Moreover, it was also ruled that the intermediary benefitted financially from advertisements on the website. Lastly, it was found that the intermediary did not take reasonable steps to prevent and avoid infringements.[111] South Korea's Copyright Act classifies intermediaries into four categories and provides the same safe harbour as the DMCA allows.[112] It, however, allows for another limitation on liability when it is technologically impossible for the intermediary to take measures and meet the conditions required. The notice and take down mechanisms are similarly modelled.[113]

Other states have adopted similar treatments. In Singapore, the Copyright Act provides that safe harbour defences apply to intermediaries providing services and connections for data transmission or routing, as well as intermediaries who provide or operate facilities for online services or network access.[114] Israel's law on copyright introduces the concept of an "innocent infringer." In the Copyright Act of 2007, such is defined as one that

---

[108] 17 U.S.C. § 512(d).
[109] EC Directive, *supra* note 15, art. 14.
[110] § 116AH(1).
[111] Cooper v. Universal Music Australia Pty. Ltd. [2006] FCAFC 187, Dec. 18, 2006.
[112] Copyright Act, *last amended by* Act No. 12137 (Dec. 30, 2013), art. 102.
[113] *Id.* art. 103.
[114] Copyright Act (amended Jan. 31, 2006), § 193A.

did not know, or could not have known, at the time of the infringement, that copyright subsists in the work. In this case, it shall not be obligated to pay compensation in respect of the said infringement.[115]

Furthermore, it should be noted that in recent cases, the European Court of Justice had the opportunity to provide guidance in the application of the EC Directive. With regard to blocking orders, the court has provided a standard to determine if such may be considered as "reasonable": "(i) they do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right."[116] As to linking, the court has held that there is no difference between a link which takes the user to another website where the work is lawfully displayed and one which embeds the work, giving the impression that it is appearing on the linking website.[117] Lastly, as to filtering, it was held that the "relevant intellectual property laws must be read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights." Hence, a national court is precluded from issuing an injunction against a hosting service provider which requires it to install a system for filtering: "(1) information which is stored on its servers by its service users; (2) which applies indiscriminately to all of those users; (3) as a preventative measure; (4) exclusively at its expense; and (5) for an unlimited period, (6) which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright."[118]

4.2. Defamation

A law on defamatory statements places the liability on the original source of the injurious information that bears direct liability as the "primary

---

[115] Copyright Act of 2007, § 58.

[116] Case C-314/12 UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproducktionsgesellschaft mbH (ECJ, Mar. 27, 2014), ¶ 63.

[117] Case C-466/12 Nils Svensson v. Retriever Sverige AB (ECJ, Feb. 13, 2014).

[118] Case C-70/10 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (ECJ, Nov. 24, 2011); also in Case C-350/10 Uitgevers CVBA (SABAM) v. Netlog NV (ECJ, Feb. 16, 2012).

speaker."[119] Generally, the following elements must be proved: (a) false and defamatory statement concerning another; (b) communication of the statement to a third party; (c) fault amounting to at least negligence; and (d) actionability of the statement irrespective of special harm.[120] From the foregoing, it can be gleaned that the essential element of a claim under defamation is publication or the communication of the defamatory statement to a third party other than the claimant.[121]

Under US jurisdiction, publishers of defamatory content are generally held liable as the primary speaker regardless of the extent of its editorial control or knowledge of the defamatory statement.[122] The rationale behind this policy is that a publisher has the knowledge, opportunity, and ability to exercise editorial control over the content of its publications.[123] On the other hand, distributors and mere conduits are held to a more limited liability. Distributors are only held liable if they have knowledge or have reason to know of a material's tortious or illegal nature and fail to stop making the material available to others or face liability for its continued publication.[124] The liability of mere conduits is similar to the liability of distributors and depends on absence of knowledge and fault.[125]

Early US cases on defamatory statements on the Internet have applied the aforementioned principles to intermediaries. In *Cubby, Inc. v. CompuServe, Inc.*,[126] it was held that the defendant, being a distributor, could not be held liable for defamatory statements in its forum. The plaintiff has to prove that the former had knowledge, actual or constructive, of the defamatory nature of the content at the time of distribution. In *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[127] the intermediary was considered to be acting as a publisher as it exercised control and supervision over the content in its forum through filtering.

---

[119] Ardia, *supra* note 1, at 394, *citing* Second Restatement of Torts § 558 (1977).

[120] *Id.*

[121] *Id.* at 396.

[122] *Id.* at 397, *citing* Harris v. Minvielle, 19 So. 925, 928 (La. 1896) and Dixson v. Newsweek, Inc., 562 F.2d 626, 631 (10th Cir. 1977).

[123] *Id. citing* Loftus Becker Jr., *The Liability of Computer Bulletin Board Operators for Defamation Posted by Others*, 22 CONN. L. REV. 203, 222 (1989).

[124] *Id.* at 398, *citing* Tacket v. General Motors Corp., 836 F.2d 1042, 1046-47 (7th Cir. 1987).

[125] *Id. citing* Dworkin v. Hustler Magazine, Inc, 634 F. Supp. 727, 729 (D. Wyo. 1986).

[126] Ardia, *supra* note 1, at 406-7, *citing* 776 F. Supp. 135 (SDY 1991).

[127] 1995 WL 323710 (N.Y. Sup. Ct. 24 May 1995).

In 1996, the US enacted CDA that, as previously noted, follows the general immunity regime.[128] § 230 of the CDA provides that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. No cause of action may be brought and no liability may be imposed under any State or local law. In effect, the CDA overturned the ruling in *Stratton* by providing intermediaries immunity in dealing with indecency. Note that in *Reno,* the anti-decency provisions of the CDA were declared as unconstitutional due to overbreadth. The US Supreme Court ruled that expression made through the Internet receives the same amount of protection as speech through traditional media. The provisions of the § 230 of the CDA failed to clearly define "indecent" communications, limit its restrictions to particular times or individuals, provide supportive statements from an authority on the unique nature of internet communications, and conclusively demonstrate that the transmission of "offensive" material and is therefore devoid of any social value.

Despite the ruling in *Reno,* § 230 remains in force. In *Blumenthal,* the intermediary was adjudged to be immune from suit even if it benefited financially from the defamatory content posted due to audience capture.[129] Nevertheless, there are some decisions that held otherwise. In *Grace v. eBay,*[130] the intermediary did not come under the purview of § 230 as it was considered to be a distributor and not a publisher. It was still, however, held to be immune as its contractual terms with its users excluded liability.

Other jurisdictions have departed from the general immunity regime that US adopted in dealing with defamation. Instead, the safe harbour regime is adopted. For instance, South Korea's Information and Communications Network Act exempts public institutions from implementing a real-name identification system from defamation-related liability.[131] On the other hand, in applying the EC Directive, the European Court of Justice has ruled the Directive does not preclude member states from adopting rules of civil liability for defamation, applicable to information society service providers established in its territory.[132]

---

[128] 47 U.S.C. § 230.

[129] 992 F. Supp. 44 (D.D.C. Apr. 22, 1998)

[130] 120 Cal. App. 4th 984, 996 (Cal. App. Ct. 2004).

[131] Information and Communications Network Act, *amended by* Act No. 11322 (Feb. 17, 2012), art. 44-5.

[132] Case C-291/13 Sotiris Papasavvas v. O Fileleftheros Dimosia Etaireia Ltd. and Others (ECJ, Sept. 11, 2014), ¶ 33.

Interestingly, in stark conflict with the *Reno* Doctrine of the US Supreme Court, the European Court of Human Rights (ECtHR) ruled in the case of *Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* that the risk of harm posed by content on the Internet is higher than that posed by the traditional media. Hence, the policies governing material on printed media and the Internet will clearly differ, the "latter undeniably adjusted according to the technology's specific features."[133] This is directly inconsistent with the decision of the US Supreme Court in finding that the Internet received the same amount of protection from that given to traditional media.

In other states, the treatment of intermediary liability in relation to defamation depends on the extent of control on the content. For instance, in the United Kingdom, an intermediary is not considered the primary speaker, editor, or publisher of a defamatory statement if it is only involved as the operator of or provider of access to a communication system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.[134] In the case of *Godfrey v. Demon Internet,*[135] the defence of innocent dissemination was found not to be available to the intermediary due to the actual knowledge it has received of the defamatory statement in its newsgroup. In Australia, an instance of hyperlinking was ruled to have amounted to a publication of the defamatory imputations in the hyperlinked webpage as it conveyed to the user that the intermediary considered the imputations in the hyperlinked article to be part of a complete version of events.[136] In a lower court decision, search engines were considered as publishers of the defamatory material if their software produce and put together search results in accordance with its intended operation.[137]

In the case of *Delfi AS v. Estonia,* the applicant company was found to have exercised two general mechanisms to review comments posted in their webpage: an automatic system of deletion of comments based on stems of vulgar words; and a notice-and-take-down system where anyone could report inappropriate comments by simply clicking on a button designated for that purpose. In addition to these mechanisms, Delfi AS also proactively moderated comments made. The European Court found that Delfi AS, as the

---

[133] Editorial Board of Pravoye Delo and Shtekel v. Ukraine, (ECtHR, May 5, 2011).

[134] Gavin Sutter, The Evolution of Liability for third Party Provided Content in the UK (17th BILETA Annual Conference, Amsterdam, Apr. 2002), *citing* Defamation Act 1996 (1996 c. 31).

[135] [2001] QB 201.

[136] Visscher v. Maritime Union of Australia (No. 6) [2014] NSWSC 350, Mar. 31, 2014.

[137] Trkulja v. Google Inc. [2012] VSC 533, Nov. 12, 2012.

provider, obtained the "technical or manual measures to prevent defamatory statements from being made public." In light of its exercise of control over its content, Delfi AS was adjudged liable for the defamatory comments made on its webpage as it was in a "position to know about an article to be published, to predict the nature of the possible comments prompted by it and, to take measures to prevent defamatory statements from being made."[138]

4.3. Deceptive of Misleading Information

Intermediaries have also been held liable for content that deceptive or misleading. In Australia, § 52 of Trade Practices Act of 1974 provides that: "[a] corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive." In relation to this, § 85(3) states: "[i]n a proceeding in relation to a contravention of a provision of Part V [...] committed by the publication of an advertisement, it is a defence if the defendant establishes that he or she is a person whose business it is to publish or arrange for the publication of advertisements and that he or she received the advertisement for publication in the ordinary course of business and did not know and had no reason to suspect that its publication would amount to a contravention of a provision of that [p]art."[139]

In *Google Inc. v. Australian Competition and Consumer Commission,*[140] the High Court of Australia ruled that Google did not engage in deceptive or misleading conduct by displaying or publishing misleading "AdWords" in organic search results. It was determined that Google was not the author of these sponsored links and merely displayed the advertisement through an automated response system. Google did not adopt nor endorse the representations made by advertisers. Hence, it was not relevantly different to physical intermediaries who publish, display or broadcast others' advertisements.

4.4. Illegal or Harmful Content

Liability for the distribution of illegal or harmful content through the Internet is governed differently compared to that of copyright infringement and defamation. Moreover, the conditions for such imposition depend on the nature of the content and the relative harm it may cause users. This section will discuss how liability is imposed on the intermediary based on different materials, namely: obscenity, child pornography, hate speech and terrorism.

---

[138] Delfi AS v. Estonia App. No. 64569/09 (ECtHR, Oct. 10, 2013).

[139] Both provisions had been superseded by § 18(1) and § 251 of the Australian Consumer Law, Schedule 2 to the Competition and Consumer Act 2010.

[140] (2013) 249 CLR 435; [2013] HCA 1, Feb. 6, 2013.

4.4.1. Obscenity

In the United Kingdom, content is considered obscene if it has the tendency to "deprave or corrupt" those exposed to it.[141] Generally, possession of an obscene article is not an offence with the exception of paedophilic content.[142] What is considered as an offence is possession with the intention of publication for gain.[143] To date, there had been no claims brought against intermediaries in the United Kingdom.[144]

Obscenity it treated differently in the US. There, the test for what may be considered as obscene had been provided in the case of *Miller v. California*[145] which laid down a three-point test: (a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. However expansive the test is, § 230 of the CDA is what is considered to be applicable to intermediaries. While there are attempts to remedy this situation, none has been successful to this date. In 1998, the US passed the Child Online Protection Act (COPA) for the purpose of purpose of restricting access by minors to any material defined as harmful to them on the Internet. This, however, was ruled to be unconstitutional in the case of *Ashcroft v. ACLU*.[146] There, the US Supreme Court held that there were less restrictive alternatives to COPA including blocking and filtering software. Hence, intermediaries are granted general immunity in relation to obscene content. In 2009, a US court has held that based on § 230 of the CDA, hosts have immunity despite claims that one its website's section constituted a public nuisance because it caused or induced prostitution.[147]

Other jurisdictions have also placed liability on intermediaries in relation to obscene content. In Iran, the Computer Crimes Law outlaws the act of facilitating others' access to obscene content.[148] In South Korea, the Information and Communications Network Act established the Korea Communications Commission that has the power to order service providers

---

[141] R v. Anderson & Others, 3 All ER 1152 (1971).

[142] Sutter, *supra* note 134, *citing* Protection of Children Act 1978, § 1, *amended by* the Criminal Justice and Public Order Act 1994.

[143] *Id. citing* Obscene Publications Act 1964 § 1(2).

[144] *Id.* at 2-3.

[145] 413 U.S. 15 (1973).

[146] 535 U.S. 564 (2002).

[147] Dart v. Craigslist Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009).

[148] Computer Crimes Law (June 2009), § 15.

to reject, suspend, or restrict processing of illegal information that includes, among others, obscene content.[149] In a 2006 case, the South Korean Supreme Court was faced with the issue of whether employees of an intermediary had the duty to delete obscene materials on the Internet. The Court found the employees of a hosting service to have abetted the crime by nonfeasance as they failed to remove obscene cartoons in their web-portal.[150]

4.4.2. Child Pornography

In the US, due to the sensitive nature of child pornography, greater responsibility is placed on the part intermediaries.[151] In 1990, the US enacted the Protection of Children from Sexual Predators Act that required service providers to report evidence of child pornography. [152] Intermediaries, however, have still been held to have immunity under § 230 of the CDA. In *Doe v. AOL*,[153] the intermediary was held not to be liable for monitoring a chat room containing obscenities. In *Doe v. GTE Corp.*,[154] the intermediary was held not to be liable for disseminating a secretly filmed video of minors. Lastly, in *Doe v. MySpace*,[155] the court held that § 230 grants immunity to intermediaries for "ineffective security measures."

In the United Kingdom, the Protection of Children Act of 1978 criminalises the taking, distribution, exhibition, or possession of children's indecent photographs.[156] This was further strengthened by the Criminal Justice and Public Order Act 1994.[157] Lastly, the Sexual Offences (Conspiracy and Incitement) Act of 1996 criminalised the act of storage of child pornography on the Internet.[158]

In 2001, the Council of Europe adopted the Budapest Convention that in turn took effect in 2004.[159] One of the content-related offenses under the convention is that of child pornography that includes the intentional

---

[149] Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., *last amended by* Act No. 11322, Feb. 17, 2012.

[150] Supreme Court Decision 2003Do4128, Apr. 28, 2006.

[151] Frydman & Rorive, *supra* note 7, at 51.

[152] 42 U.S.C. § 13032.

[153] 718 So 2d 385 (4th Cir. 1999).

[154] 347 F.3d 655 (7th Cir. 2009).

[155] 528 F.3d 413 (5th Cir. 2008).

[156] Protection of Children Act of 1978 (1978 c. 37).

[157] Criminal Justice and Public Order Act 1994 (1994 c. 33), § 84.

[158] Sexual Offences (Conspiracy and Incitement) Act of 1996 (1996 c. 29).

[159] Budapest Convention (Budapest Convention on Cybercrime); Forty-five member states have ratified the Convention along with the United States of America, Canada, South Africa and Japan.

commission of the following acts: "(a) producing child pornography for the purpose of its distribution through a computer system; (b) offering or making available child pornography through a computer system; (c) distributing or transmitting child pornography through a computer system; (d) procuring child pornography through a computer system for oneself or for another person; (e) possessing child pornography in a computer system or on a computer-data storage medium."[160] Additionally, pornographic material that visually depicts the following are also considered within the purview of the article: "(a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; and (c) realistic images representing a minor engaged in sexually explicit conduct."[161] The liability of an intermediary falls under the definition of "aiding and abetting" defined in article 11 of the Convention. Based on the explanatory report,[162] however, a service provider that does not have the requisite criminal intent cannot incur liability under this section. This may imply that, there is no duty under this section for an ISP to actively monitor content in order to avoid criminal liability under this section.

Other state regulators have enacted similar laws. Kenya's Sexual Offenses Act of 2006 prohibits child pornography that involves distribution and receiving profits from distribution of obscene materials to a child.[163] South Korea's Act on the Protection of Children and Juveniles Against Sexual Abuse holds intermediaries liable for failure to take measures prescribed to detect child or juvenile pornography or for failure to immediately delete the detected pornography and take technical measures to prevent or block transmission thereof.[164] In South Africa, intermediaries are mandated to take all reasonable steps to prevent the use of their facilities for the hosting or distribution of child pornography. The law also requires intermediaries to report to legal authorities the presence of such material along with particulars to aid in investigations.[165] Finland's application of the law is more restrictive. In a decision of its Supreme Court in 2013, an intermediary was held to liable for propagating child pornography by providing links of blocked targets.[166]

---

[160] Budapest Convention (Budapest Convention on Cybercrime, art. 9(1).

[161] Art. 9(2).

[162] Explanatory Report of the Commission of Ministers of the Convention on Cybercrime, 109th Session (adopted on Nov. 8, 2001), ¶ 119.

[163] Sexual Offences Act of 2006 (amended by Act No. 12 of 2012), § 14.

[164] Act on the Protection of Children and Juveniles Against Sexual Abuse (amended by Act No. 11690, Mar. 23, 2013), art. 17.

[165] Film and Publications Act (Act No. 65/1996, Nov. 8, 1996), § 27.

[166] Supreme Administrative Court, Lapsiporno.info, KHO 2013:136 (Aug. 26, 2013). The ruling was based on Act 1068/2006 (Measures Preventing the Propagation of Child pornography, Dec. 2006).

4.4.3. Hate Speech

There is no general trend in imposing liability on the intermediary for material containing hate speech or incitement to violence. After all, a state policy regarding hate speech and incitement to violence seems to be determinative of its approach toward such content. Hence, under the free speech principle, the liability depends on a case-by-case basis that takes into consideration the factual circumstances of a particular jurisdiction and an analysis of the grave and substantial harm that may be caused by the act of the intermediary in hosting such content.[167]

American jurisprudence recognises that the right to freedom of expression guarantees a "marketplace of ideas" where people may freely discuss ideas of public interest.[168] Moreover, it has been held that this is a necessary condition for the realization of the principles of transparency and accountability that are essential for the promotion and protection of human rights.[169] Speech is protected merely by virtue of it being speech. Even the advocacy of religious hatred is considered protected speech as the right to freedom of expression includes the right to express extreme views.[170] That the ideas being expressed are repugnant to the general public or to specific groups does not mean that they do not contribute to the "free interchange of ideas."[171] Even views that do not conform to generally accepted opinions promote diversity of thought necessary to a free society.[172] Hence, the State cannot restrict expression because of its message or ideas[173] though they may tend to "offend, shock or disturb"[174] for these are, "within established limits, [... but are] necessary side effects"[175] of the right of free expression.

While speech that merely amounts to advocacy of hatred is accorded the same level of protection as other types of speech, the same is not true

---

[167] Stephen Newman, *Should Hate Speech Be Allowed on the Internet?*, 2 AMSTERDAM L. FORUM 119, 123 (2010).

[168] Abrams v. Unites States, 250 U.S. 616 (1919) (Holmes, J., *dissenting*); *see also* Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., *concurring*); Terminiello v. Chicago, 337 U.S. 1 (1949); Knox v. Service Employees, 132 S. Ct. 2277 (2012).

[169] Hertzberg and Others v. Finland, Communication no 61/1979 UN Doc CCPR/C/15/D/61/1979 (1983).

[170] New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

[171] Garrison v. Louisiana, 379 U.S. 64 (1964); Gertz v. Welch, 418 U.S. 323 (1974).

[172] Cox v. Louisiana, 379 U.S. 536 (1965).

[173] Police Department of Chicago v. Mosley, 408 U.S. 92, 95 (1972).

[174] Handyside v. United Kingdom, App. No. 5493/72 (ECtHR, Dec. 7, 1976); Stankov and the United Macedonian Organisation Ilinden v. Bulgaria, Apps No 29221/95 and 29225/95 (ECtHR, Oct. 2, 2001).

[175] Cohen v. California, 403 U.S. 15 (1971).

when due to the speech uttered gives rise to clear, present, and imminent threats of serious evil which the state has a right to protect.[176] Therefore, when the aim of the offensive words is to spread violence or hatred, resort to illegal or undemocratic methods, or pursue objectives that are racist or likely to destroy the rights and freedoms of others, these are considered not to be protected and may be validly suppressed. The burden, however, is on the State to demonstrate the precise nature of the threat in the speech as well as a direct and immediate connection between the expression and the threat.[177]

On the other hand, the EU presents a different perspective. Under the European Convention on Human Rights, the exercise of the right to freedom of expression carries with it "special duties and responsibilities," including "respect for the rights or reputations of others."[178] Hence, states may lawfully suppress such speech that are only gratuitously offensive and do not contribute to public debate.[179] Incitement to hatred is considered to communicate threats to commit acts of unlawful violence to particular individuals and groups latter of their rights and freedoms, or to disrupt public order.[180] Furthermore, such incitement against particular groups promotes intolerance and discrimination is considered to have "serious and damaging consequences" in multicultural and pluralist societies.[181]

Based on the rulings of the European Court of Human Rights, the right to freedom of expression may be restricted, provided the restriction in question passes a "three-fold test." First, the interference with the right must be "prescribed by law." This requires that the regulation must have an adequate basis in domestic law that it be "adequately accessible" and "formulated with sufficient precision." Second, the interference must be in pursuit of a legitimate aim, such as, *inter alia,* an interest of national security, or public safety. Third, the restriction must pass the test of proportionality and must be "necessary in a democratic society." [182] Notably, in the

---

[176] Gitlow v. New York, 268 U.S. 652 (1925); Brandenburg v. Ohio, 395 U.S. 444 (1969).

[177] *Id*; Hess v. Indiana, 414 U.S. 105 (1973).

[178] European Convention on Human Rights (adopted Nov. 4, 1950; entered into force Sept. 3, 1953), art. 10.

[179] Handyside v. United Kingdom, App. No. 5493/72 (ECtHR, Dec. 7, 1976); Wingrove v. United Kingdom, App. No. 17419/90/90 (ECtHR, Nov. 25, 1996); Feret v. Belgium, App. No. 15615/07 (ECtHR, July 16, 2009).

[180] Ceylan v. Turkey, App. No. 23556/94 (ECtHR, July 8, 1999); Prosecutor v. Nahimana (Appeal), ICTR-99-52-A (ICTR, Nov. 28, 2007).

[181] UNHRC, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Ambeyi Ligabo, A/HRC/7/14 (2006).

[182] The Sunday Times v. The United Kingdom, App. No. 6538/74 (ECtHR, Apr. 26, 1979).

determination of what is considered necessary and proportional, states are accorded a "margin of appreciation" allowing it to derive a "balance between the protection of the general interest of the community and the respect due to fundamental human rights while attaching particular importance to the latter."[183] Following this test, states are permitted to regulate the freedom of expression following a determination of a "pressing social need" after taking into consideration the audience of such speech.[184]

The EC Directive allows member states to restrict the freedom to provide information society services from another member if such act is necessary based on the state public policy, "in particular the prevention, investigation, detection and prosecution of criminal [offences], including the [...] fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons."[185] The Council of Europe also sought to criminalise hate speech and incitement to violence. Under the Additional Protocol to the Budapest Convention,[186] acceding states are encouraged criminalise the following activities: dissemination of racist and xenophobic material through computer systems; racist and xenophobic motivated threat, racist and xenophobic motivated insult; and denial, gross minimisation, approval or justification of genocide or crimes against humanity.[187] Like the Budapest Convention, the Additional Protocol includes a provision on criminalising "aiding and abetting" that may be applicable to intermediaries.[188]

EU member states have applied the same treatment in the determination intermediary liability. In a 2000 case,[189] the French High Court ordered Yahoo Inc. to take all measures to prevent Internet users in France from accessing auctions sales of items promoting Nazism or denying crimes

---

[183] Belgian Linguistics Case (No. 2), App. Nos. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63, and 2126/64 (ECtHR, July 23, 1968); Handyside v. United Kingdom, App. No. 5493/72 (ECtHR, Dec. 7, 1976.

[184] Erdogdu and Ince v. Turkey, App. Nos. 25067/94 and 25068/95 (ECtHR, July 8, 1999); Vajnai v. Turkey, App. No. 33629/06 (ECtHR, July 8, 2008); Vejdeland v. Denmark, App. No. 1813/07 (ECtHR, Feb. 9, 2012).

[185] EC Directive, *supra* note 15, art. 3(4).

[186] Additional Protocol to the Convention on Cybercrime (concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems).

[187] Additional Protocol to the Convention on Cybercrime (concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems), art. 3-6.

[188] Art. 7.

[189] Frydman & Rorive, *supra* note 7, at 46, *citing* LICRA v. Yahool, No RG:00/0538 (Nov. 22, 2000).

committed during the Nazi period. In a later case,[190] the actions of an intermediary hosting Nazi and other racist sites was held to violate not only the French law but also the European Convention for the Protection of Human Rights together with the Universal Declaration of Human Rights. In Switzerland, federal police placed the aforementioned host in the "black list" which is voluntarily blocked by Swiss intermediaries.[191]

4.4.4. Terrorism

In the recent years, the Internet has been used to further acts of terrorism it being a highly dynamic means of communication and because of its reach to an ever-growing audience worldwide. In 2012, the UN Office on Drugs and Crime ("UNDOC") identified six categories in which the Internet is being used to further terrorist activities: "propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyberattacks." [192] As part of its policy recommendations, the UNDOC stated that part of the answer to the prevalence of terrorism-related activities in the Internet is to enact measures allowing for the "regulation of Internet-related services and content control."[193] Specifically, the office recommended that a "universally agreed regulatory framework imposing consistent obligations on all ISPs regarding the type and duration of customer usage data to be retained would be of considerable benefit to law enforcement and intelligence agencies investigating terrorism cases."[194]

Other jurisdictions have also recognised the role on intermediaries in relation to terrorist activities. In the United Kingdom, the Terrorism Act of 2006 allows the police to require providers of electronic services to remove terrorist statements or articles that are being hosted on the Internet. In case of failure to do so without reasonable excuse, the institution may be deemed to have endorsed the statements and senior officers may be liable for criminal prosecution.[195] In Russia, a resolution was adopted in 2014 pursuant to the anti-terrorism package of bills. This resolution establishes that intermediaries: (a) should identify Internet users, by means of identity documents and to (b)

---

[190] *Id.* at 49, *citing* J'Accuse decision (Oct. 30, 2001).

[191] *Id.*

[192] United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes, 3 (2012).

[193] *Id.* at 134.

[194] *Id.* at 138.

[195] Terrorism Act 2006 (2006 c 11), § 3(1).

identify terminal equipment by determining the unique hardware identifier of the data network. Moreover, all legal entities in Russia are required to provide intermediaries monthly with the list of the individuals that connected to the Internet using their network.[196] In a lower court decision in Turkey, a blocking order related to the display of acts of violence and terrorism was issued to block videos depicting terrorist propaganda and attacks. This was issued in relation to the Turkish Anti-Terror Law.[197]

5. PHILIPPINE CONTEXT

5.1. Philippine Laws on Intermediary Liability

Currently, the country has three laws relating to the subject of intermediary liability: the Electronic Commerce Act of 2000,[198] the Anti-Child Pornography Act of 2009,[199] and the Cybercrime Prevention Act of 2012.[200] There are also two pending bills in the Philippine Senate—Bill Nos. 53 and 1091—that seek to enact the Magna Carta for Philippine Internet Freedom.

5.1.1. Electronic Commerce Act

The Electronic Commerce Act was enacted with the view of facilitating efficient domestic and international electronic transactions. It primarily applies to data message and electronic document used in the context of commercial and non-commercial activities.[201]

Under said law, an "intermediary" is defined as "a person who in behalf of another person and with respect to a particular electronic document sends, receives and/or stores or provides other services in respect of that electronic document."[202] The law, however, separately defines a "service provider" which refers to "on-line services or network access, or the operator of facilities therefor, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing."

---

[196] Resolution of the Government of the Russian Federation on July, 31 2014.
[197] Turkish Anti-Terror Law. No. 3713.1, §§ 6-7.
[198] Rep. Act. No. 8792 (2000).
[199] Rep. Act. No. 9775 (2009).
[200] Rep. Act. No. 10175 (2012).
[201] Rep. Act. No. 8792 (2000), §§ 3-4.
[202] § 5(h).

As to the liability of "service providers," they are immune from civil and criminal suits relating to the obligations and responsibilities of parties based on the electronic data. For "the making, publication, dissemination or distribution of such material or any statement made in such material," however, they must satisfy three conditions.[203] First, the service provider must not have actual knowledge or is not aware of the facts or circumstances from which it is apparent relating to the illegality of the material. Second, it must not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity. Third, it must not directly commit any infringement or other unlawful act and does not induce or cause another to do the same.[204]

5.1.2. Anti-Child Pornography Act of 2009

The Anti-Child Pornography law was enacted by the Philippine congress as a response to prevailing incidents relating to child pornography, as well as to comply with international treaties to which the Philippines is a signatory or a state party concerning the rights of children.[205]

The law distinguishes between hosts and service providers. Under § 3(f), an "[I]nternet content host" is defined as "a person who hosts or who proposes to host [I]nternet content in the Philippines." The law mandates that the host shall not store or allow storage in its facilities of "any form of child pornography." Furthermore, the law requires hosts to report the presence of any form of child pornography and the particulars of the party related to such activity. Hosts are penalised for knowingly, intentionally, and wilfully violating these requirements. While the law does not provide for a take down clause, it treats the failure of the host to remove any form of child pornography to be a conclusive evidence of wilful and intentional violation thereof.[206]

On the other hand, an ISP, as defined in § 3(g), is a person or entity that supplies or proposes to supply, an internet carriage service to the public. Under the law, it has the responsibility of providing the authorities with information on activities relating to child pornography committed using its server or facility. Furthermore, it has the duty of preserving any evidence for purpose of investigation and prosecution by relevant authorities. Lastly, it is mandated to "install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered."[207]

---

[203] § 30.
[204] § 30.
[205] Rep. Act No. 9775 (2009), § 2.
[206] § 11.
[207] § 9.

5.1.3. Cybercrime Prevention Act of 2012

The Cybercrime Prevention Act of 2012 was enacted by the Congress recognizing that "cyberspace is a boon to the need of the current generation for greater information and facility of communication" and that it is difficult to "filter out a number of persons of ill will who would want to use cyberspace technology for mischiefs and crimes." It was enacted in exercise of the government's legitimate right to "to regulate the use of cyberspace and contain and punish wrongdoings."[208]

The Cybercrime Prevention Act defines "service provider" as "any public or private entity that provides to users of its service the ability to communicate by means of a computer system" and "any other entity that processes or stores computer data on behalf of such communication service or users of such service."[209] While providing for acts or omissions considered to crimes within the purview of the law, the service providers are considered liable if it "wilfully abets or aids in the commission of any of the [offences] enumerated in this Act shall be held liable."[210] Furthermore, the law penali es service providers if it fails to fulfil the following duties: (a) preserve computer data within a specified period; and (b) disclose such traffic data and subscriber information after being compelled to do so by authorities.[211]

5.1.4. Magna Carta for Philippine Internet Freedom

Recognizing perhaps the deficiency of the Electronic Commerce Act of 2000, the Anti-Child Pornography Act of 2009, and the Cybercrime Prevention Act of 2012, the Senate sought to enact the Magna Carta of Philippine Internet Freedom. Senate Bill Nos. 53 and 1091 were filed in July 2013 and after consolidation, are currently pending before the Philippine Senate. Both bills seek to address the problem of network sabotage, violation of data privacy and security, infringement of intellectual property rights, Internet libel, hate speech, child pornography, and cyber-terrorism.[212] At the same time, the bills seek to protect the freedom of speech and expression on the Internet and the public's universal access.[213] Furthermore, the said bill seeks to amend existing laws, among others the Public Telecommunications Act and the Intellectual Property Code, insofar as allowing them to cater to

---

[208] Disini v. Secretary of Justice, G.R. No. 203335, 716 SCRA 237, Feb. 11, 2014.
[209] Rep. Act. No. 10175 (2012), § 3(n).
[210] § 5(a).
[211] §§ 13-14.
[212] S. No. 53, §§ 43, 45-6, 48, 52-3.
[213] §§ 4-5.

the demand of the Internet. As to intermediaries, the said bills make a distinction, akin to the other jurisdictions, pertaining to mere conduits, caching service providers, information locators, and hosting service providers.

5.2. Analysis

In Part III, it has been submitted that the more appropriate approach in dealing with intermediary liability broadly is that of the vertical approach because it places less burden on the part of the intermediary. Furthermore, based on the specific regimes, it has been argued that the most reasonable regime is that of safe harbour as it tends to balance the responsibilities of intermediaries and the burden that it has to discharge. In Part IV, the different areas of regulation have been examined and it was shown that these different areas require different regimes based on the harm that the content may cause. In Part II, it was discussed that the different natures of intermediaries (mere conduits, information locator tools, caching service providers, and host service providers) require different standards of liabilities. Hence, in the analysis of Philippine intermediary laws, the following matters will be determined: first, the applicable liability regime, second, the application on each area of substantive law as juxtaposed to trends relating the same area of law in other jurisdictions; and third, the standards based on the nature of the intermediaries.

5.2.1. Regime of Liability

The regime followed by the three Philippine laws suggests that of safe harbour. The three laws require knowledge on the part of the intermediary of the act or omission before liability is attached. In the Cybercrime Prevention Act, the aiding and abetting must be done wilfully. Otherwise, liability cannot be imposed upon the intermediary.[214] The same is required under the Anti-Child Pornography Act. Under said law, the activities of the host that may give rise to liability must be committed "knowingly, intentionally, and wilfully."[215] Lastly, under the Electronic Commerce Act, the intermediary must have actual knowledge or must be aware of the facts or circumstances from which it is apparent relating to the illegality of the material,[216] similar to that standard of the EC Directive. As previously discussed, said law abides by the conditional liability regime, which requires prior notice or knowledge on the part of the intermediary.

---

[214] Rep. Act No. 10175 (2012), § 5(a).
[215] Rep. Act No. 9775 (2009), § 11.
[216] Rep. Act No. 8792 (2000), § 30.

Compared to other jurisdictions, the three laws seem to fall short of providing a specific notice and take down procedure. The DMCA requires a specific form of notice before the host may be required to remove a particular material from their servers. This includes: (a) the name, address and electronic signature of the complainant; (b) sufficient information to identify the material; (c) the infringing matter and its location; (d) a statement by the complainant that it has a good faith belief that there is no legal basis for the use of the materials complained of; and (e) a statement of the accuracy of the notice and, under penalty of perjury.[217] The reason behind this requirement is to sufficiently appraise the host that it is hosting an illegal or harmful material, that the information they received has a basis, and that it they may face liability for taking down or disabling access to a content that turns out to be legal.[218] While the laws requires knowledge on the part of the intermediary, this lack of notice and take down procedure may cause a chilling effect, and consequently, would have the intermediaries assume the function of a censorship body: in order to avoid liability intermediaries would opt to take down a content upon allegations of infringement or illegality.[219]

The Cybercrime Prevention Act does not provide for such notice. Under said law, the liability attaches to intermediaries if it "wilfully abets or aids in the commission of any of the [offences] enumerated in this Act shall be held liable."[220] Under said procedure, prior notice of the illegality of the content or conduct is inessential in the imposition of liability on the intermediary. The determination of its liability rests on whether its act of aiding or abetting is wilful in nature.

The same problem may be found in the Electronic Commerce Act. There, intermediaries may only be held liable for material stored if they: (a) have actual knowledge or is aware of the facts or circumstances from which it is apparent relating to the illegality of the material; (b) knowingly receives a financial benefit directly attributable to the unlawful or infringing activity; (c) directly commits any infringement or other unlawful act and does not induce or cause another to do the same.[221] The law, however, does not provide for any mechanism under which the intermediary may be sufficiently informed of it acts or omissions that may constitute violations of the said law.

---

[217] 17 U.S.C. § 512(c).
[218] Baistrocchi, *supra* note 23, at 124.
[219] *Id.* at 130.
[220] Rep. Act No. 8792 (2000), § 20.
[221] § 30.

The Anti-Child Pornography Act similarly suffers from the same problem, albeit at a lesser extent. Liability attaches to the hosts and service providers if, upon the request of proper authorities, they fail to furnish the particulars of users who gained access to an Internet address that contain any form of child pornography.[222] The law, however, fails to specify the nature and kind of notice that the intermediary should receive.

The Magna Carta for Philippine Internet Freedom seems to address this problem. In promoting the freedom of use of the Internet, the bill provides that the State should "not promote censorship or the restriction of the viewing of any content on the Internet, until after the issuance of an appropriate Order."[223] Furthermore, it is stated that "any State action that constitutes prior restraint or subsequent punishment in relation to one's Internet's rights shall be authorised only upon a judicial order issued in conformity with the procedure provided."[224] The judicial order may be issued upon finding of the following grounds: "(i) the nature of the material or information subject of the order creates a clear and present danger of a substantive evil that the State has a right or duty to prevent; (ii) the material or information subject of the order is not protected expression under the standards of the community or the audience toward which the material or information is directed; and (iii) the publication of the material or the uploading of the information subject of the order will constitute a criminal act punishable by laws enumerated [in the Act]."[225] The proposed law also takes into consideration the control that the intermediary exercises over the content: "[n]o person shall be compelled to remove published content or uploaded data from the Internet that is beyond the said person's capacity to remove. The party seeking to compel the removal of the content or data has the burden to prove that the person being compelled has the capacity to remove from the Internet the specific content or data [...] [C]ontent or data retained in web archives or mirror sites are presumed to be content and data that is beyond the capacity of the person being compelled to remove."[226]

The aforementioned Philippine legislations, however, fail to provide for a "put back" procedure. Under this mechanism, the owner of the material alleged the be illegal or harmful may request that the content removed be replaced or access be re-enabled by the intermediary upon proof that the content does not infringe on the rights of others or is not otherwise illegal. As

---

[222] Rep. Act No. 9775 (2009), §§ 9(2)(i), 11(1)(i)(c).
[223] S. No. 1091, 16th Cong., 1st Sess., § 4(a)(iv) (2013).
[224] § 4(c).
[225] § 4(c).
[226] § 4(d).

previously discussed, this procedure affords a more complete protection for all the actors involved. It provides owners of content a remedy to restore access to their content. Also, it allows for safeguards against false claims of illegality and harm. Lastly, it shields that intermediary from liability if it can claim "good faith [in] 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, regardless of whether the material or activity is ultimately determined to be infringing."[227]

5.2.2. Areas of Regulation

The Philippine laws on intermediary liability deal with following areas of regulation: copyright, child pornography, and cybercrimes. It does not seem, however, to address other areas of regulation that other jurisdictions have responded to, such as terrorism, defamation, and hate speech.

Regarding terrorist activities on the Internet, no Philippine law has been enacted in order to address this concern. Note that the UNDOC, due to the prevalence of terrorism-related activities in the Internet, has recommended that as a policy, measures have to be enacted for the "regulation of Internet-related services and content control."[228] As previously stated, the office recommended that there must be "universally agreed regulatory framework imposing consistent obligations on all ISPs regarding the type and duration of customer usage data to be retained would be of considerable benefit to law enforcement and intelligence agencies investigating terrorism cases."[229] Currently, such measures are in place in countries including but not limited to: United Kingdom, Russia, and Turkey. Nowhere in the Cybercrime Prevention Act, Electronics Commerce Act, or Anti-Child Pornography Act is the act or omission related to terrorist activities penalised. Similarly, no liability attaches to the intermediary in the event that it becomes a tool for such activities. Such provision, however, may be found in the Magna Carta for Philippine Internet Freedom insofar as it penalises the commission of offences found in the Human Security Act of 2007 and Terrorism Financing, Prevention and Suppression Act of 2012 when committed on the Internet.[230]

---

[227] 17 U.S.C. § 512(h).

[228] United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes, 134 (2012).

[229] *Id.* at 138.

[230] S. No. 53, 16th Cong., 1st Sess., § 53(b) (2013).

Similar to the terrorist activities on the Internet, currently, there are neither Philippine law nor jurisprudence that touches on the issue of hate speech disseminated through the Internet. As such, the liability of the intermediary hosting hate speech related content is left undefined. In other jurisdictions, it was previously demonstrated that the treatment of hate speech, differs based on the policy of the state. Under US jurisprudence speech that merely amounts to advocacy of hatred is accorded the same level of protection as other types of speech but the same is not true when due to the speech uttered gives rise to clear, present, and imminent threats of serious evil which the state has a right to protect.[231] The treatment is different in the EU. The EC Directive allows member states to restrict the freedom to provide information society services from another member if such act is necessary based on the state public policy that includes the "fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons."[232] The Council of Europe also sought to criminalise hate speech and incitement to violence under the Additional Protocol to the Budapest Convention.[233] Note however, under the Magna Carta for Philippine Internet Freedom Bill, hate speech on the Internet, defined as a "public and malicious expression calling for the commission of illegal acts on an entire class of persons, a reasonably broad section thereof, or a person belonging to such a class, based on gender, sexual orientation, religious belief or affiliation, political belief or affiliation, ethnic or regional affiliation, citizenship, or nationality, made on the Internet or on public networks" may only be punishable if the expression "calls for the commission of illegal acts on the person or class of persons that, when they are done, shall cause actual criminal harm to the person or class of persons, under existing law" and "when commission of illegal acts [poses] an immediate lawless danger to the public or to the person who is the object of the expression."[234]

Lastly, with regard to defamation, as previously discussed the treatment of the issue differs based on the policy of the state. The US adheres to the general immunity regime, as reflected under § 230 of the CDA where no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. Furthermore, no cause of action may be brought and no liability may be imposed under any State or local law. Other states on the other hand, such as those in the EU, have adopted a safe harbour regime under

---

[231] *Gitlow*, 268 U.S. 652; *Brandenburg*, 395 U.S. 444.

[232] EC Directive, *supra* note 15, art. 3(4).

[233] Additional Protocol to the Convention on Cybercrime (concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems).

[234] S. No. 53, 16th Cong., 1st Sess., § 52(b) (2013).

which intermediary liability in relation to defamation may be imposed, in light of the circumstances. These may include prior notice, such as that expressed in the EC Directive, or the extent of control on the content hosted, as considered in the case of *Delfi AS v. Estonia* previously discussed.

In the Philippines, libel committed on the Internet is penalised under the Cybercrime Prevention Act. Under said act, libel on the Internet is defined as the "unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future." [235] The said provision was upheld to be constitutional insofar as it penalises the original author of the post, but was declared to be unconstitutional with respect to others who simply receive the post and react to it.[236] As with the other offences enumerated under the said law, the intermediaries may be considered liable if it wilfully abets or aids in the attempt to commit or the commission of offence.[237]

Under the Magna Carta for Philippine Internet Freedom, Internet libel is defined as "a public and malicious expression tending to cause the dishonour, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead, made on the Internet or on public networks."[238] Said bill further provides that Internet libel shall not lie if malice or intent to injure is not present and that positive identification of the subject as an essential element of internet libel.[239] From this proposed bill, it may be argued that Philippine legislation is leaning towards a safe harbour regime, for while prior notice may not be expressly required by its provisions, the same nonetheless necessitates actual knowledge. This is similar to the standard imposed under § 19(a)(i) of the EC Directive that requires either actual knowledge of unlawful activity or awareness of facts or circumstances from the illegality of the content may be gleamed.

To require malice or intent, and wilfulness as aforementioned, however, may clash with the view advocating the constructive notice standard. As previously discussed, the actual knowledge standard, or in this case, the requisite of intent and wilfulness, would lead to a low risk of liability for the intermediary. As a result, it provides the intermediary an incentive to not monitor the content hosted in its facilities, or in fact, to feign ignorance as to

---

[235] S. No. 53, 16th Cong., 1st Sess., § 4(c)(4) (2013).
[236] *Disini*, 716 SCRA 237.
[237] Rep. Act No. 10175 (2012), § 5.
[238] S. No. 53, 16th Cong., 1st Sess., § 52(a) (2013).
[239] § 52(a)(ii)-(iii).

the knowledge and illegality of conduct and content hosted. Applying the constructive knowledge approach negates this possibility since the standard imposes a higher risk of liability for intermediaries, and thus forces them to enact mechanisms to avoid liability.[240] The same could be said under the gross negligence standard.

5.2.3. Nature of Intermediaries

Finally, it seems that Philippine intermediary laws fail to distinguish between the natures of different intermediaries or worse, fail to address the liability of other types of intermediaries. The three laws consider mere conduits. Hosting service providers, however, are contemplated only under the Cybercrime Prevention Act and the Anti-Child Pornography Act. Such is not addressed in the E-Commerce Act. Notably, the Anti-Child Pornography Act differentiates between the "intermediaries" and "service providers." After providing the definition for "intermediaries," however, nowhere is the term found anywhere in the law. In the succeeding sections, it merely provides for the extent of liability of "service providers." Moreover, information locators and caching services that also play a big role in facilitating different activities on the Internet are left completely unaddressed.

The Magna Carta for Philippine Internet Freedom seems to attempt to address this problem insofar as recognizing the delineation among Internet service providers,[241] caching service providers,[242] information locators,[243] and hosting service providers.[244] The proposed bill, however, still falls short in providing for specific kinds of liabilities considering the nature of these intermediaries. In comparison, the DMCA and EC Directive provides for specific instances under which a mere conduit, caching service provider, information locator, or hosting service provider may be deemed liable.

6. CONCLUSION

The Philippine laws dealing with intermediary liability seem to have been a step towards implementing a system that seeks to respond to the prevalence of illegal, harmful, or otherwise infringing content on the Internet while providing a proportionate burden on the part of the intermediaries.

---

[240] S. No. 53, 16th Cong., 1st Sess., § 52(a)(ii)-(iii) (2013).

[241] S. No. 1091, 16th Cong., 1st Sess., §§ 9(c), 10(c), 36(b), 37(a), 37(c), 38(c), 44(a), 44(c), 45(a), 45(c) (2013).

[242] §§ 3(f), 38(e).

[243] §§ 38(c), 38(e).

[244] § 38(c).

Nevertheless, the loopholes present numerous problems that would impede the implementation of the said laws and fails to take into consideration technical developments and Internet practices. These problems seemed to have been addressed by the regulations of other States including the EC Directive and the DMCA. By taking into consideration these practices, Philippine intermediary laws may be properly amended if only to secure the use of the Internet within the State.

In light of the pending Magna Carta for Philippine Internet Freedom, future legislation may take into consideration the practices of foreign states with regard to prior notice, actual knowledge, and constructive knowledge. As the law stands today, prior notice is not required, but only wilfulness in the act. This, however, is not in line with the safe harbour regime that is recognised as the standard most in line with the right to freedom of expression. This regime requires prior notice before the imposition of liability.

Before pursuing any further development, the Philippines must further define its policy with regard to the right to free expression online. As previously discussed, different jurisdictions have dissimilar, and sometimes contrasting policies as to the protection given to online speech. In *Reno*, the US Supreme Court recognised that expression made through the Internet receives the same amount of protection as speech through traditional media. On the other hand, the European Court of Human Rights has ruled under a less liberated policy. In the cases of *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* and *Delfi AS v. Estonia*, the court found that "the risk of harm posed by content on the Internet is higher than that posed by the traditional media"[245] because "information once made public will remain public and circulate forever"[246] and therefore calls for caution. With "the ease of disclosure of information on the Internet and the substantial amount of information,"[247] regulation of the Internet must be "adjusted according to the technology's specific features."[248]

With Internet law as relatively unchartered territory, Philippine legislation must first look to its roots before moving forward. To define the very policy behind our regulation to date, whether they be liberal or restrictive, would be the first step to developing necessary and proportional regulations for the legislation to come.

---

[245] Editorial Board of Pravoye Delo and Shtekel v. Ukraine, (ECtHR, May 5, 2011); Delfi AS v. Estonia App. No. 64569/09 (ECtHR, Oct. 10, 2013).

[246] *Id.*

[247] *Id.*

[248] *Id.*