Jurisdictional Analysis

Comparative Study Of Intermediary Liability Regimes
Chile, Canada, India, South Korea, UK and USA
in support of the Manila Principles On Intermediary Liability

Version 1.0, 1 July 2015

Authors and Affiliations

Jyoti Panday
(Programme Officer) Centre for Internet and Society, India

J. Carlos Lara
(Research and Policy Manager) Derechos Digitales, Chile

Kyun S Park
(Professor) Korea University Law School;
(Director) Open Net, Korea

Kelly Kim
(General Counsel) Open Net, Korea

Acknowledgements

The author would like to the inputs and feedback of Rishabh Dara, Jeremy Malcolm, Gabrielle Guillemin, Shradha Nigam, Elonnai Hickok, Pranesh Prakash and Sunil Abraham.

Declaration of Conflicting Interests

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this analysis.

Funding

Research, authorship, and/or publication of this article and the development of the Principles has been generously funded by a grant from MacArthur Foundation.

Permissions

The author has sought permission from the Steering Committee developing the Manila Principles and members who have contributed to this analysis.

Corresponding Author

Jyoti Panday,
Centre for Internet and Society
Top Floor, G-15 Hauz Khas
New Delhi 110016
INDIA
Email: jyoti@cis-india.org

Abstract

Governments around the world undertake speech regulation through the imposition of liability on intermediaries for third-party content, and often impose related obligations of proactive monitoring, exercising due diligence, and other such requirements. This study highlights the trends and crucial differences in existing liability regimes across Chile, Canada, India, South Korea, UK and USA. This analysis has been undertaken by the steering committee developing the Manila Principles and is aimed at supporting the development of the Manila Principles - a global civil society initiative.

Keywords

Intermediary liability, freedom of expression, regulation of platforms, Internet Service Providers (ISPs), monitoring

Table of Contents

1 Introduction

The realization of the freedom of opinion and the freedom of expression online necessarily requires interacting with 'Internet intermediaries'. These may be corporations that provide Internet access, those that provide domain names, and platforms hosting content, enabling online search, or providing a wide variety of other services and functions. Because of the critical role they play in facilitating the viewing and access to content online, intermediaries become crucial points for the government who impose liability on intermediaries for third-party content. As part of this regulation, governments may impose obligations of proactive monitoring and exercising due diligence for intermediaries in relation to third party content.

For freedom of expression to thrive on the Internet, it is essential to establish safe harbours protecting intermediaries from liability over content that they did not create or edit. This paper deals with the approaches to the regulatory treatment of intermediaries for third party content that may be deemed harmful.

This study seeks to highlight trends and crucial differences across existing liability regimes towards supporting the Manila Principles (hereinafter referred to as Principles). The Principles are a high level framework that seek to inform legislation, policies, norms, practices that relate to filtering, restricting, removing and blocking third party content by an intermediary. This study stresses the practical need for the Principles, given the various classes of intermediaries, widely varying procedures and conditions that impose liability and different criteria that qualify the intermediary for immunity across existing liability regimes. The jurisdictions included in the study are Chile, Canada, India, South Korea, UK and USA.

Across many jurisdictions, there is no one legislation guiding the legal regime regulating content restrictions imposed on intermediaries. Across regimes that regulate removal of content, governments can have separate legal provisions based on different criteria and standards that allow for restricting content online. Courts also establish standards on a case by case basis, and there are other technological and policy developments that shape content restriction practices and liability for intermediaries e.g., right to be forgotten, data protection and other issues that could have implications for intermediaries.[1]

In recent years, there have been several attempts to map and compile the law and case law applicable to intermediaries including cross jurisdictional analysis, most notably the Stanford World Intermediary Liability Map[2], reports from Centre for Democracy and Technology

[1] MacKinnon Rebecca, Hickok Elonnai, Bar Allon, and Lim Hae-in, Fostering Freedom Online, The role of Internet Intermediaries, UNESCO series on Internet Freedom, UNESCO (2014). See: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

[2] World Intermediary Liability Map at Center For Internet and Society at Stanford. See more he available at: http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap

(CDT)[3], and United Nations Educational Scientific and Cultural Organization (UNESCO)[4]. There is a pressing need to extend this area of comparative research to include temporal mapping.

Thus, this analysis has been attempted as a temporal approach, mapping the evolution of liability regimes and content restriction practices across the identified jurisdictions. There are two reasons why such temporal comparative research is needed. Firstly, most intermediary liability regimes are relatively new, with the oldest having been introduced merely fifteen years ago.[5] The nascent and evolving regulatory landscape makes it crucial to map the evolution and history of how law regulating online intermediaries is being institutionalized and how interpretation varies not only across countries and but also over time. Such analysis is critical to refining our understanding of the shift in regulatory regimes that may arise across jurisdictions and over time. Secondly, given the evolution of technology, if policymaking is to keep pace with the issues that arise with advances in online communication, legislation must acknowledge and assess the limitations of current frameworks and learn from existing practices across countries.

2 Methodology

2.1 Approach to analysis

This study follows the "functional approach"[6] in legal comparative research which assesses primarily the function of a specific norm regardless of its national categorisation. There are several reasons why this approach has been selected towards comparing different liability regimes.

First, with the focus of functionalist comparative law on the effects of rules and events, it leads away from doctrinal structures. This approach considers judicial responses to real life situations and legal regimes which are then compared to various judicial decisions on similar issues. Second, the functionalist approach to comparative law is grounded in the theory that law and society are separable but related, and that object of study must be understood in light of their functional relation to society. Third under this approach, legal and nonlegal

[3] Shielding the Messengers: Protecting platforms for expression and innovation, Version 2, updated December 2012. See here: https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

[4] MacKinnon, supra note 3

[5] Ronald J. Mann, Seth R.Belzley, "The Promise of Internet Intermediary Liability", Volume 47 | Issue 1, William & Mary Law Review, accessed June 10, 2015 See: http://www.arl.org/focus-areas/copyright-ip/2486-copyright-timeline#.VXgb69_vZCU

[6] Kennedy David, '*New Approaches to Comparative Law: Comparativism and International Governance*', Utah L. Rev. 545 (1997). See: http://heinonline.org/HOL/LandingPage?handle=hein.journals/utahlr1997&div=31&id=&page=

institutions across different legal regimes may be compared as long as they fulfill a similar function—thus the function itself serves as *tertium comparationis*. Fourth, the function can serve as an evaluative criterion and help us understand laws that fulfill their objective better than others.

The study is aimed at identifying the common trends and crucial differences in the assessment of notions and concepts of intermediary liability. Unique trends in countries are important as they may be considered as blueprint for other countries when confronted with the same issues. It is important to bear in mind that this functionalist comparison does not presume that different solutions to similar problems are really 'similar'. Solutions may vary in their doctrinal structures, or in their effects and functions or dysfunctions regarding the problem. Rather, the approach presumes functional equivalence—that different solutions are similar regarding one element, addressing the issue at hand.

2.2 Structure of the study

This study has been conducted to illuminate emerging trends and opportunities for strengthening approaches to imposing liability on intermediaries. The Principles define some of the safeguards and best practices that are essential for a balanced intermediary liability framework. Towards systematically comparing implemented frameworks, we have identified categories for comparison and developed criteria and indicators expanding on the categories, in consultation with international experts. The categories and criteria for comparison have been developed as to map the different components of existing liability regimes across jurisdictions. Good and bad practices from implemented regimes so as to develop normative benchmarks or standards that are essential to developing a balanced liability regime. The analysis aims to capture the multiple components of intermediary liability within each country and the methodology applies a two-pillared approach to understanding the frameworks in place.

Under this two-pillared approach we distinguish liability provisions that stipulate certain conditions following which intermediaries may claim immunity, or place additional obligations not related to immunity on the intermediary. We have also distinguished if the liability regime provides immunity from voluntary takedowns and we outline the different procedures set in place for content restriction and removal such as notice and notice (NTN) and notice and takedown (NTD).

To highlight the complexity of content restriction practices in place across countries, we also consider provisions placing additional liability for intermediaries such as complying with executive orders and private complaints. Through the two-pillared lens, the methodology examines intermediaries' role in relation to two broad groupings: unlawful content and user information with nearly 30 subpoints accompanying the groupings.

The purpose of the sub-points is to guide researchers and policymakers regarding the procedural elements and safeguards that they should consider when evaluating and implementing liability frameworks. After developing the criteria, it was used to compare applicable legislation across India, Canada, the United Kingdom and the United States of America. This comparative grid was shared with the steering committee for review and feedback and independent counsel and review was also sought from academics working in this area of research.

During the review period, the committee reviewed, critiqued, and adjusted groupings and criteria after careful consideration of the laws, practices and issues relevant to each country. Upon completion of the categorisation, committee members from Chile and South Korea added the relevant data completing the analysis. The steering committee did a final review to ensure comparative reliability and the completed grid was presented at the launch of the Manila Principles and inputs and feedback were sought from experts present at the launch, including contributors to the Stanford WILMap.

Some of the sub-points covered while analysing procedures include actual or constructive interpretation of knowledge, locus standi, prescribed level of proof, executive or judicial notices, action to be taken upon receipt and informing users about action taken, opportunity to be heard and redressal mechanisms. Criteria related to user information include sub-points around data retention, disclosure requirements such as logging of identification details and information accessed, sharing user information with private parties through requests or court orders, and sharing information with law enforcement and/or in the interest of national security and co-operation obligations including providing assistance for interception by the government or its agents.

2.3 Presentation of the study

This approach was tested in a pilot edition, analysing existing frameworks across selected countries and this has been presented as a grid. We have expanded on the analysis of the grid in a detailed narrative across two sections in this paper. The first section provides an introduction to liability frameworks and existing models across regimes. The section also introduces legal instruments that create either conditional immunity or provisions that place additional liability. We also elaborate on the legal claims addressed, the procedures outlined, and the types of intermediaries covered under each framework.

The second section evaluates the legal measures adopted across the selected countries to understand if the legislation adequately balances legitimate priorities such as appeal, redress and transparency. Together, both sections examine and outline the law in place across each country and what has guided the legislation in place for each jurisdiction. The study touches upon the implementation of the liability regimes, including similarities and differences across the interpretation and implementation of standards that relate to intermediary liability.

3 Regulatory approaches to intermediary liability

The Internet has evolved into a global network providing unprecedented access to, and dissemination of, information and services without any territorial or time limits. While this proliferation of technology has enabled the use of information for economic and educational purposes, it has also led to the creation and dissemination of certain content which may be unlawful, cause harm to, or impinge on the rights of others.

Given that potentially unlawful or harmful content on the Internet may be widespread and difficult to curtail, intermediaries are under increasing pressure from government and interest groups to act as online 'gatekeepers'. Governments regulate online intermediaries by establishing obligations and procedures through a liability regime. Intermediary liability is not a peculiarity of internet law. It represents a standard feature in fiduciary relationships governed by employment and insurance law, as well as banking and securities regulation.[7] It has also often been invoked in intellectual property (IP) cases even before the internet era concerning a form of intermediation impacting on the commercial use of a product.[8]

3.1 Carriage and content

Essentially, there are two elements that any intermediary liability framework seeks to regulate- the carriage of communications and the content of communications. The first element, carriage of communications considers legal provisions and procedures with respect to the intermediaries' function as a facilitator of that communication. Balanced liability procedures and guidelines should seek to go beyond this broad understanding and consider the nature of this facilitation and the specific function of the intermediary.

The second element, content of communication, considers legal provisions in relation to pre-defined or specified content. It is important to note that liability may appear in relation to many different types of content. For example, unlawful information dissemination on the Internet may take the form of defamation and one of the earliest case in the USA addressing the issue of hosting libelous content was Cubby v CompuServe[9]. Liability frameworks have also developed around copyright and related issues and cases such as Napster[10], Grokster[11],

[7] Nicolo Zingales, Internet Intermediary Liability, Identifying Best Practices for Africa. See: https://www.apc.org/en/system/files/APCInternetIntermediaryLiability_BestPracticesAfrica_20131125.pdf

[8] *Ibid. 6*

[9] In *Cubby*, CompuServe argued that it was a distributor and not a publisher and therefore could not be liable for the content because it did not know and had no reason to know about the statements in question. See Cubby, Inc. v. CompuServe Inc. 776 F.Supp. 135 (S.D.N.Y. 1991), Internet Library of Law and Court Decisions, *available at*:http://www.internetlibrary.com/cases/lib_case69.cfm.

[10] So called Napster case is a landmark intellectual property case in which the United States Court of Appeals for the Ninth Circuit affirmed the ruling of the United States District Court for the Northern District of California, holding that defendant, peer-to-peer file-sharing service Napster, could be held liable for contributory infringement and vicarious infringement of the plaintiffs' copyrights. This was the first major case to address the

and MegaUpload[12] are examples where private online intermediaries as litigating parties have raised the fast changing nature of technology to avoid liability.

For intermediaries, liability for failure to block, filter and remove expression online, may also arise in relation to content that is deemed obscene and harmful.[13] There exist varying approaches to the regulation of hate speech across countries, for example in US hate speech[14] is assimilated into political speech and is granted utmost protection by the Supreme Court. In India, Article 19(1)(a) guaranteeing the right of all citizens 'to freedom of speech and expression', is not an absolute right and, is subject to Article 19(2), that must be exercised in a way that does not jeopardize the rights of another or clash with the 'paramount interest of the State or community at large'.[15]

In some countries certain types of information is also curtailed arising from public policy decisions[16]. Section R645-1 of the French Penal Code that criminalize the exhibit or display of Nazi emblems and artifacts and prohibit dissemination of information that "may be construed as constituting an apology for Nazism or a contesting of Nazi crimes" was the basis for the famous proceedings against Yahoo Inc[17]. Increasingly, national security, terrorism, and cyber security are reasons being incorporated into legal regimes for removal of content.[18]

3.2 Vertical and horizontal frameworks of regulation

Presently, most liability regimes do not contain incentives for intermediaries to not restrict content, and two broad models in regulating intermediaries have emerged. The first, is a

---

application of copyright laws to peer-to-peer file-sharing. See US case: A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[11] Mere knowledge of infringing potential or of actual infringing uses or ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability are not enough to subject a distributor to liability. The inducement rule premises liability on purposeful, culpable expression and conduct that does nothing to compromise legitimate commerce. See US case: MGM Studios, Inc. v. Grokster, Ltd. 545 U.S. 913 (2005).

[12] TechDirt MegaUpload Case Summaries See more: https://www.techdirt.com/?company=megaupload

[13] Pg 29-56, Zittrain and Palfrey, Internet Filtering: The Politics and Mechanisms of Control, Access Denied, 2008, The MIT Press

[14] Hate speech is a controversial term, see Article 19, 'Prohibiting incitement to discrimination, hostility or violence', December 2012. See more:http://www.article19.org/data/files/medialibrary/3548/ARTICLE-19-policy-on-prohibition-to-incitement.pdf

[15] Liang Lawrence, '*Free Speech and Expression*', upcoming volume edited by Pratap Bhanu Mehta et al, Oxford Handbook of Constitutional Law in India

[16] Council of Europe's Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, See: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

[17] Elissa A. Okoniewski, 'Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1189&context=auilr

[18] Kelly Sanja, Earp Madeline, Reed Laura, Shahbaz Adrian, Mai Truong, 'Tightening the Net: Governments Expand Online Controls', Freedom on the Net, 2014, See: https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

'horizontal' framework that differentiates between the classes and functions of intermediaries for the purpose of limitation of liability, and sets out a framework in relation to all type of content.[19] Under such horizontal approach, the system of liability exemptions is applicable no matter what the nature of interests at stake.

It is important to bear in mind, that the horizontal approach, regardless of the type of content in question differs in its application and interpretation across jurisdictions. For example, the legislation in European Union (EU)[20] defines class specific liability for intermediary based on the function and type of intermediary. The Indian liability regime applicable to all types of content, does not clearly distinguish between the various types of intermediaries or account for the various functions that intermediaries perform in processing and storing communications online.[21]

Countries may also adopt a 'vertical' framework where they limit liability for intermediaries for specific content or issues at stake. Canada's and Chile's liability regime has developed around the issue of copyright. UK has separate legislation for defamation, India has outlined a separate liability framework for copyright and the US includes copyright infringements and associated intermediary liability under the Digital Millennium Copyright Act (DMCA)[22].

Countries may also enact multiple legislations, provisions and procedures to restrict unlawful content. In South Korea liability on issues of copyright, telecommunications, juveniles and election related issues is dealt with under different legislations specifically, Copyright Act[23], Telecommunications Business Act (TBA)[24], Act on the Protection of Children and Juveniles against Sexual Abuse[25], Act on Consumer Protection in Electronic Commerce[26], Information

---

[19] Centre for Democracy and Technology report, 'Shielding the messengers', Version 2 (updated December 2012) See:https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031

[21] Arun, Chinmayi and Singh, Sarvjeet, Online Intermediaries in India (February 18, 2015). NOC Online Intermediaries Case Studies Series. Available at SSRN: http://ssrn.com/abstract=2566952

[22] Digital Millennium Copyright Act 1998, 17 U.S.C. § 512 See: http://www.law.cornell.edu/uscode/text/17/512

[23] Copyright Act, Amended by Act No. 9625, Apr. 22, 2009; Act No. 10807, Jun. 30, 2011; Act No. 11110, Dec. 2, 2011 http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25455&lang=ENG

[24] Telecommunications Business Act No.12035, Enforcement Date 14. Feb, 2014 13. Aug, 2013., Partial Amendment http://www.law.go.kr/lsInfoP.do?lsiSeq=142966&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

[25] Act on the Protection of Children and Juveniles Against Sexual Abuse, last amended by Act No. 11690, March 23, 2013 See: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=28311&lang=ENG

[26] Act on the Consumer Protection in Electronic Commerce, Etc., last amended by Act No. 11461, June 1, 2012 See: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25650&lang=ENG

and Communications Network Act (ICNA)[27], the Public Official Election Act (POE Act)[28] and Act on Establishment and Operation of Korean Communication Commission[29]. In Chile, Law No. 20. 453 deals with intermediaries' non-interference and Law No. 20. 435 establishes limitations on the liability of the ISPs for copyright

A recurring theme that emerges in our evaluation, regardless of the approach to framing regulation, is that the intermediaries are often put in the role of an adjudicator and, are forced to take decisions on what content is legal and which is not. This creates a paradox, where intermediaries, with no legal competence decide on the legality of the action and because determining this is not a priority, often simply block access to, or remove the alleged unlawful content.

3.3 Models and procedures for intermediary liability

Adopting laws that hold private intermediaries financially or criminally responsible for failing to filter, block or remove unlawful content on behalf of the state or for private interests, without appropropriate accountability measures and safeguards leads to broad censorship. On the other hand, the lack of legislative protection for liability, may impose demanding negligence standards or lead to strict interpretations of what constitutes negligence on the part of the intermediary. A lack of a regime protecting online platforms from liability under certain circumstances has serious implications on freedom of expression and speech online as often, intermediaries will err on the side of caution and take down lawful content[30]. China[31] and Thailand[32] are examples of countries with *'no legislative protection'* from liability and where intermediaries are held liable for third party content and are effectively, required to monitor

[27] Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (ICNA, Information and Communications Network Act), last amended by Act No. 11322, February 17, 2012. See: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG

[28] Public Official Election Act, last amended by Act No. 11071, November 7, 2011 See: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25035&lang=ENG

[29] Act on the Establishment and Operation of Korea Communications Commission, Amended by Act No. 11711, Mar. 23, 2013 See: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=28155&lang=ENG

[30] Dara Rishabh, *'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet'*, Centre for Internet and Society (2011) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038214

[31] Art 10. The Copyright Law of the People's Republic of China was amended for the first time in 1990, and for the second time in 2010. This consolidated version of the Copyright Law incorporates all amendments up to the Decision of February 26, 2010, of the Standing Committee of the National People's Congress on Amending the Copyright Law. See: http://www.wipo.int/wipolex/en/details.jsp?id=6062

[32] Sections 15 of the Computer Crimes Act BE 2550 (Thailand, 2007), English translation available at http://advocacy.globalvoicesonline.org/wp-content/plugins/download-monitor/download.php?id=2; see also Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, "Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai-State Policies ," iLaw Project, December 8, 2010, http://www.boell.de/downloads/ilaw_report_EN.pdf. A draft revision to the CCA, released in 2011, but not adopted as of this writing, would similarly create criminal liability for intermediaries; see CDT, Comments on Thailand's Proposed Computer-Related Offenses Commission Act, March 2012, https://www.cdt.org/files/pdfs/Comments-Thailand-CCA-Draft.pdf

and restrict content.[33] Under such models of regulation failure to comply with the law, may lead to intermediaries facing criminal prosecution or withdrawal of license for operating their business in these countries.

Across other countries internet intermediaries are provided *'broad immunity'* from liability for a wide variety of third-party content and exempted from any general requirement to monitor content. The broad immunity model found in USA[34] and European Union (EU)[35] distinguishes intermediaries' role in relation to content for example, intermediaries are distinguished as 'publishers' post-notification, who are responsible for the content that they disseminate, although it is produced by others.[36] Other classes of intermediaries are treated as 'messengers,' and not held responsible for the content they carry or transmit.

Other countries have adopted a third model that limits liability for online intermediaries for third party content and provides *'conditional immunity or safe harbour'*[37]. Under this safe harbour model, an intermediary receives protection from liability for user conduct, only if the intermediary complies with certain criteria and meets certain conditions such as compliance with statutory 'notice and notice' (NTN) or 'notice and takedown' (NTD) procedures.[38] This model seeks to balance the need for limiting liability, while defining certain role or procedures for intermediaries in relation to unlawful content. Under this model, the immunity for intermediaries may also be conditional to them complying with prescribed procedures and actions in relation to users who are repeat offenders. One such procedure that sets out obligations for restricting repeated infringements that has developed specifically in relation to copyright infringement is the 'graduated response' approach.[39]

3.4 Procedures outlined under liability frameworks

There are important distinctions amidst the NTD, NTN procedures and a 'graduated response' approach. Typically, NTD regime create a system of incentives or require an ISP to block access to material upon receipt of a notice from a rights holder alleging illegality of material or content. The obligation to restrict or block access lies with the intermediary and it is not necessary that there is a requirement of a court order to take down infringing content. The NTD procedure have been enacted in US under the DMCA, and in India, under the

[33] Internet Intermediaries: Dilemma of Liability, Article 19, See: http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

[34] Section 230 under Communications Decency Act, 1996 See:http://www.law.cornell.edu/uscode/text/47/230

[35] Directive 2000/31/E *supra note* 22

[36] Not a publisher pre-notification. See Tamiz v. Google the Court of Appeal verdict http://www.scl.org/site.aspx?i=ed31376

[37] Pg 40, MacKinnon, *supra note* 3

[38] MacKinnon, *supra note* 3

[39] Lovejoy Nathan, *'Procedural Concerns with the HADOPI Graduated Response Model'*, HARVARD Journal of Law and Technology, Edited by Harry Zhou (January 2011). See: http://jolt.law.harvard.edu/digest/copyright/procedural-concerns-with-the-hadopi-graduated-response-model

Intermediary Rules (2011) of the Information Technology (Amendment) Act 2008[40] and the Copyright Act of 1957, as amended by the Copyright (Amendment) Act 2012[41]. South Korea also provides for NTD under Art 103, Copyright Act.

Implementation of NTD may vary across countries, for example in Chile under Law No. 20.453 a NTD procedure, under which a court order is required — instead of a private notice – to have content taken down.[42] Initially, in India the NTD procedure did not mandate court orders for restriction of impugned content by the intermediary in order to seek exemption from liability, though this has recently been read down.[43]

In South Korea, copyright law has been revamped to establish the NTD procedure as a compliance standard for safe harbor though under other laws such as ICNA or the Public Officials Election Act, NTD is procedure established as an outright obligation. Child sex protection laws and the TBA, establish monitoring obligations for intermediaries for restricting child pornography and obscene material online. The monitoring obligations outlined under the liability framework do not relate to conditional immunity related to safe harbour which intermediaries may choose to forgo, rather these are stipulated conditions which have to be met as an absolute duty.

On the other hand, the *vertical* approach may also be implemented through a NTN procedure for restricting infringing or unlawful third party content. As followed in Canada[44], NTN requires intermediaries to forward any notice of infringement they receive from copyright owners, to the subscriber in question.

The NTN procedures differ from NTD in two major ways. First, the NTN procedure, as enacted under the Copyright Modernization Act (CMA) 2012 in Canada, does not provide a

[40] Information Technology (Intermediaries guidelines) Rules, (2011) to be read with read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000)
See: http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

[41] The Copyright (Amendment) Act, 2012 See: http://www.wipo.int/edocs/lexdocs/laws/en/in/in066en.pdf

[42] For a fuller description of the Chilean law and a summary of the process that led to its adoption, see Daniel Alvarez Valenzuela, "The Quest for Normative Balance: The Recent Reforms to Chile's Copyright Law," International Centre for Trade and Sustainable Development, December 2011, http://ictsd.org/i/publications/120938/.

[43] Panday Jyoti, 'The Supreme Court Judgment in Shreya Singhal and What It Does for Intermediary Liability in India?', ORF Cyber Monitor, 2015 April
See:http://www.orfonline.org/cms/export/orfonline/html/cyber/Cyber_Monitor_0415.pdf

[44] Copyright Modernization Act, SC 2012, c 20. Canada. See: http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/page-1.html

duty for online service providers to take down allegedly infringing content. Second, ISPs are granted a safe harbour independently of their compliance with the NTN procedure.[45]

Across countries that follow a conditional immunity model, either conditions could be adopted as a preferred standard that grants safe harbor independent of compliance with procedure or in accordance with compliance to the outlined procedure. Following the two-pillared approach, it is worth considering that both the NTN and NTD procedures or a graduated response scheme, may stem as provisions for conditional immunity or as provisions that impose additional obligations that do not contribute to the immunity of the intermediary.

3.5 Graduated response scheme as due diligence

Regimes may also impose due diligence requirements or obligations, including but not restricted to, dealing with repeated offenders who post unlawful content online through the *graduated response approach*. Such regimes outline obligations ranging from issuing warnings, collating allegations made against subscribers and reporting to copyright owners, suspension and eventual termination of service as actions which the intermediary must take to be able to claim immunity.[46] Graduated response schemes may vary in their implementation and usually, formal legislative schemes contain more safeguards for due process than privately negotiated contracts in place.

In France, for example, after an initial administrative scheme, known as HADOPI, was held to be unconstitutional by the French Constitutional Council[47], a new system was introduced which requires a full criminal proceeding for disconnection for periods up to one year[48]. In 2013 the law was overturned and replaced with a system of automatic fines.[49] In UK the graduated scheme had been developed as a legislatively supported industry code to be enacted under Digital Economy Act 2010 (UK) c 24.[50] However, subsequent proposed regulations

[45] Francois Joli-Coeur, 'Canada's Approach to Intermediary Liability for Copyright Infringement: the Notice and Notice Procedure', Berkley Technology Journal, March 2, 2014. See: http://btlj.org/2014/03/02/canadas-approach-to-intermediary-liability-for-copyright-infringement-the-notice-and-notice-procedure/

[46] Giblin Rebecca, '*Evaluating Graduated Response*', University of Monash, June 12 2014, See:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2322516

[47] Loi n° 2009-1311 du 28 octobre 2009 [Law No 2009-1311 of 28 October 2009] (France) JO, 29 October 2009, 18290 art 7, amending Code de la Propriété Intellectuelle [Code of Intellectual Property](France) L 335–7.

[48] *Ibid.*

[49]Siraj Datoo, The Guardian , France drops controversial 'HADOPI law' after spending millions. See:http://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy

[50] Digital Economy Act 2010 c. 24 See: http://www.legislation.gov.uk/ukpga/2010/24

fleshing out operation of the scheme and funding were held following a legal challenge to the Act.[51]

The graduated response scheme has developed in South Korea through Articles 113-2 and 133-3, Copyright Act. In the US, Motion Picture Association of America (MPAA) and five major US internet service providers launched their 'six strikes' Copyright Alert system in February 2013 to deal with online piracy.[52] The voluntary system has been launched by ISPs with the main aim of educating the public on their connections being used for copyright infringement and informing them as to where they can seek legal alternatives. Under this system, alerts start out in a friendly tone and increase in severity for repeated infringements and regular offenders may face temporary disconnection of their Internet service or other "mitigation measures".[53]

It is not clear yet what mitigation measures were used or how many subscribers were affected and concerns have been raised regarding the lack of knowledge on what penalties are applicable or how they were implemented.[54] Further, it should also be noted that some jurisdictions do not have specific legal provisions[55] addressing intermediary liability, but do issue court or executive orders for the restriction of content, as well as placing obligations including monitoring, reporting and technical obligations on service providers via operating licences.

3.6 Country specific liability framework—history and scope

3.6.1 United Kingdom

The United Kingdom was the first European country to specifically adopt legislation limiting online intermediary liability[56], following a vertical framework concerned only with defamation

---

[51] Digital Economy Act copyright regime shelved by UK government, Outlaw.com, 24 Jul 2014, See: http://www.out-law.com/en/articles/2014/july/digital-economy-act-copyright-regime-shelved-by-uk-government/

[52] Hruska Joel, *'Six Strikes' programs from ISPs & MPAA ignites in nine days: Here's what you need to know'*, Extreme Tech, (November 19, 2012). See: http://www.extremetech.com/internet/140774-six-strikes-programs-from-isps-mpaa-ignites-in-nine-days-heres-what-you-need-to-know

[53] Ernesto, 'Six Strikes results show high number of persistent pirates', May 28 2014 See: https://torrentfreak.com/six-strikes-results-show-high-number-of-persistent-pirates-140528/

[54] Stoltz Mitch, *'Six Strikes Copyright Alert System Can't Be The Future of Copyright Enforcement Without More Transparency and Accountability'*, Electronic Frontier Foundation, (June 2, 2014). See: https://www.eff.org/deeplinks/2014/06/six-strikes-needs-transparency-accountability

[55] Alice Munyua, Grace Githaiga and Victor Kapiyo Intermediary Liability in Kenya, Kenya ICT Action Network (KICTANet), Intermediary Liability in Africa Research Papers No. 2, See: https://www.apc.org/en/system/files/Intermediary_Liability_in_Kenya.pdf

[56] Horeebeek Van Mark, Law, Libraries and Technology, pg 70, Chandos Publishing (Oxford) Limited. See:https://books.google.co.in/books?id=bumiAgAAQBAJ&pg=PA70&lpg=PA70&dq=uk+defamation+first+intermediary+liability+legislation&source=bl&ots=8GLVGmjhF7&sig=80uR27NK8GHmCLV1aN8UipIFshE&hl=en&sa=X&ei=OC3LVOX1I8THmwXJoYKQDw&ved=0CFIQ6AEwCA#v=onepage&q=uk%20defamation%20first%20intermediary%20liability%20legislation&f=false

issues. UK defamation law as a general rule places liability on the publisher of a defamatory statement, that is, where an institution maintains control over what it users publish, it is likely to be considered a *"publisher"* of this material for the purpose of defamation.[57] The *Defamation Act* of 1996[58] introduced an "*innocent dissemination*" defence for distributors of hard copy publications, as well as online service providers and internet access providers. It exempted online intermediaries from liability for third party materials, provided they could prove to have taken reasonable care with respect to the publication, and did not have any reason to believe that they had contributed to the publication of a defamatory statement. The judgment in 1999, *Godfrey v Demon*[59] became the first UK case to find that such a defense would not hold for ISPs upon receiving actual knowledge of the defamatory statement having been made and led to much debate[60] on the potential liability of online service providers.

Codifying the law on defamation made up of common law supported by 1952 and 1996 Defamation Acts, the Defamation Act 2013[61] entered into force on January 1, 2014. While the Act's effect is limited to England and Wales, Section 5 creates a new defence for the operators of websites where user generated content has been defamatory[62], if intermediaries did not publish the materials themselves[63]. However, the defence is not be available if the claimant cannot not hold the website user responsible; or if the defendant upon notification of the publication fails to respond to that notice in the manner prescribed by applicable regulations. Section 5 of the Defamation Act 2013 were supplemented by the Defamation (Operators of Websites) Regulations 2013[64] came into force at the same time as Section 5 of the Defamation Act 2013. These regulations specify the characteristics of a valid notice of infringement, and the actions that an operator may take in response to complaint in order to maintain section 5(2) defence.

UK legislation also establishes conditional immunity for online intermediaries following a horizontal approach for liability in relation to all type of content. This approach differentiates between the classes and functions of intermediaries for the purpose of limitation of liability.

---

[57] JISC Legal, Hosting Liability Overview, 'Liability for Defamation', (November 23, 2007), See: http://www.jisclegal.ac.uk/LegalAreas/HostingLiability/ISPLiabilityOverview.aspx

[58] Defamation Act 1996 c. 31. See:http://www.legislation.gov.uk/ukpga/1996/31/contents

[59] Godfrey v Demon Internet Ltd, QBD, [1999] 4 All ER 342, [2000] 3 WLR 1020; [2001] QB 201. See: http://www.cyber-rights.org/documents/godfrey_decision.htm

[60] Demon coughs up damages in Godfrey libel case: Pays price for uncivil liberties. See: http://www.theregister.co.uk/2000/03/30/demon_coughs_up_damages/

[61] UK Defamation Act 2013 c. 26 see: http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted

[62] Section 5, Operators of websites, Defamation Act 2013. See: http://www.legislation.gov.uk/ukpga/2013/26/section/5/enacted

[63] Section 5, Operators of websites, Defamation Act 2013. See: http://www.legislation.gov.uk/ukpga/2013/26/section/5/enacted

[64] The Defamation (Operators of Websites) Regulations 2013 See: http://www.legislation.gov.uk/uksi/2013/3028/regulation/1/made

This model is based on the E-Commerce Directive (ECD) in the EU, where almost complete immunity is provided to intermediaries providing technical access to the internet such as telecommunications service providers or ISPs and to caching services.[65] By contrast, hosts have to meet set conditions such as acting *"expeditiously"* to remove or disable access to *"illegal"* information when they obtain actual knowledge of such content to claim immunity.[66]

Directives on political and economic matters of common interest are issued by the EU to member states for implementation under local laws. While several directives have been issued on Intellectual Property, the EU's approach to e-commerce and ISP liability is set forth in the *Directive 2000/31/EC*[67], whichh since its introduction has been implemented across all 27 member states.

ECD was enacted to ensure the free movement of *"information society services"*, and prior to its adoption, burdensome obligations and responsibilities were imposed on online service providers in the EU. The Directive was issued to provide clear directions and guidelines on the liability of ISPs following a German case where the Managing Director of an ISP was sentenced to prison for unknowingly holding pornographic content on its servers.[68]

Arising from the EU's ECD, and almost mirroring them, UK enacted the EC Directive Regulations 2002[69] transplanting the three liability 'safe harbours' into law. While the Directive uses the expression *"should not be liable"*, the Regulations expand on this phrase to enact horizontal safe harbour defenses for 'information service providers', exempting them from of damages, pecuniary remedy and criminal sanctions for a range of third party content.

Regulation 17 and 18 indemnify information society service providers providing transmission or access services to communication networks and store information pursuant to automatic, intermediate and temporary processes, respectively. Under the regulations service providers are not held liable as long as they did not initiate the transmission, and do not modify or interfere with information being transmitted or stored. *Regulation 19* indemnifies service providers providing information storage services if they did not have actual knowledge of unlawful activity or information and who upon being notified of alleged activity act expeditiously to remove or disable access to that information.

Member states cannot refute liability exemptions under the directive and in theory, they should go beyond this minimum threshold and set forth rules, that further extend exemptions

---

[65] Article 12 and 13, Directive on e-commerce 2000/31/EC of 8 June 2000 (ECD). See: http://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf

[66] Article 14, *Ibid.*

[67] Article 1, *Ibid.*

[68] Mueller Milton L., *'Networks and States: The Global Politics of Internet Governance'*, Pg 138, (2010) MIT Press.

[69] The Electronic Commerce (EC Directive) Regulations 2002 See: http://www.legislation.gov.uk/uksi/2002/2013/contents/made

for intermediaries. This perhaps could explain the differing approaches adopted to liability at the national level for example in under the Defamation Act 2013[70] and the Digital Economy Act (DEA) 2010[71] that introduces immunity to the intermediaries that is conditional to fulfilling certain pre-defined obligations under a graduated response approach to online piracy.

Enacted in June 2010, the DEA introduced *"graduated response"* approach setting out two procedures aimed at reducing online piracy. The first procedure outlined as *'initial obligations'*[72] establishes a process whereby rights holders may informing the ISP of users infringing on copyrighted material by sending a Copyright Infringement Report (CIR). The obligations for the ISP under this process include forwarding the CIR to the alleged user and further, if user receives more than three CIRs separated over a specific period of time the user is put on a copyright infringement list maintained by the ISP, which they are liable to share with the copyright holder. This may lead to further action by rights holders initiating infringement proceedings through injunctions to identify and penalise users.

A second procedure labelled *'obligations to limit Internet access'*[73], providing for mitigation measures to deal with repeated infringers that have crossed a certain threshold were to be implemented at the discretion of the Secretary of State, if the initial obligations regime was deemed ineffective.[74] If implemented, measures could vary from limiting the speed of the connection, preventing the subscriber from accessing certain online services, and even suspending the subscriber's connection altogether.

It should be noted that neither procedures have been implemented. Further, the Department for Culture, Media and Sport (DCMS) has stated last year that the implementation of the regime is on hold following the development of voluntary standards within the industry.[75] After a series of setbacks, the initial obligations beginning with ISPs issuing warning letters is expected to come into force in the second half of 2015.[76]

In addition to the graduated response procedures, Code 17 of the DEA 2010 provides, that the Secretary of State may introduce regulations explicitly providing the courts with an option

[70] Section 5, UK Defamation Act 2013. See: http://www.legislation.gov.uk/ukpga/2013/26/section/5/enacted

[71] Digital Economy Act (DEA) 2010. See: http://www.legislation.gov.uk/ukpga/2010/24

[72] DEA Sub Rule 3 Obligation to notify subscribers of reported infringements 124C or 124D An "initial obligations code". *Ibid.*

[73] DEA Code 10 Section 124 H Obligations to limit internet access. *Ibid.*

[74] DEA Code 11 124 I Subrule (6) states: 'The consent of the Secretary of State is required for the making or amendment by OFCOM of a code under this section.'

[75] Digital Economy Act copyright regime shelved by UK government, OutLaw, See: http://www.out-law.com/en/articles/2014/july/digital-economy-act-copyright-regime-shelved-by-uk-government/

[76] DEA Code 17 *Supra note* 59 http://www.completemusicupdate.com/article/uk-isps-negotiating-voluntary-strike-one-system-to-combat-piracy/

of granting a blocking injunction against a *"location on the internet"* which the court sees as *"(…) being, or (…) likely to be used for or in connection with an activity that infringes copyright."*[77]

The online service provider upon receiving the blocking injunction would have to *"prevent its service being used to gain access"* such a location. However, such regulations have not been established yet, and Code 17 itself is potentially subject to removal within the Draft Deregulation Bill 2013[78], clause 26 of which proposes omitting Code 17 and 18 of the DEA 2010.[79]

3.6.2 United States of America

The US policy on intermediary liability is enacted through two key pieces of legislations that govern intermediary liability Section 512 of the DMCA[80] and Section 230 of the Communications Decency Act (CDA).[81] The DMCA is one of the earliest legislation dealing with intermediary liability, having been introduced in 1998 and establishes a conditional immunity model under the vertical framework. DMCA lays down a *'notice-and-takedown'* (NTD) procedure specifically to address copyright infringement complaints. Section 512 of DMCA was a legislative compromise to address concerns of content escapes raised by copyright owners in the late 1990s and was originally designed as an emergency stopgap measure to be used in isolated instances, to remove infringing material from the Internet, just long enough to allow a copyright owner to get into court.[82]

The technology of the times meant that if copyright owners acted quickly enough they could prevent the spread of infringing material and the DMCA's statutory language confirm that the NTD procedure was designed as a temporary solution that was aimed at getting *"service providers and copyright owners to cooperate to detect and deal with"* infringing material. The original intent highlights the inefficiency of the procedure to deal with persistent and

---

[77] *Ibid 75*

[78] Draft Deregulation Bill, Presented to Parliament by the Minister for Government Policy and the Minister without Portfolio by Command of Her Majesty (July 2013). See: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/210035/130701_CM_8642_Draft_Deregulation_Bill.pdf

[79] Stanford WILMap: United Kingdom, See: http://cyberlaw.stanford.edu/page/wilmap-united-kingdom

[80] DMCA *supra note 23*

[81] In addition to these statutory provisions, intermediary protection may be derived from the protection of free expression granted under the Constitution. U.S. courts also have created a safe harbor from copyright infringement liability for producers and distributors of technology products under certain circumstances: 1) the product must have substantial non-infringing (that is, lawful) uses, and 2) the distributor must not have actively encouraged infringing uses of its product. Sony v. Universal Studios, 464 U.S. 417 (1984); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005).

[82] Centre for the Protection of Intellectual Property, 'The Failure of the DMCA Notice and Takedown System', George Mason University, School of Law, December 5, 2013. See: http://cpip.gmu.edu/2013/12/05/the-failure-of-the-dmca-notice-and-takedown-system-2/

ubiquitous spread of infringing content through modern technology and the costs of removing unlawful content. Importantly, DMCA provides protection to intermediaries against copyright and related claims, however not against injunctions.[83]

The other key legislation that contributes to the liability regime in US is the Section 230, Title 47 of the U.S. Code[84], providing broad immunity to intermediaries from most legal liability for user generated content (UGC). It has been interpreted broadly, across several type of unlawful content or issue at stake including in cases of defamation, privacy, negligence, and other tort claims.

Interestingly, the CDA incorporating the strongest safe harbor provisions with the broadest applicability for intermediaries arose, largely by accident. The Communications Decency Act (CDA) was introduced in February 1995, in an attempt to regulate obscenity and indecency online and despite its vague language, was tacked with telecommunications law and passed in 1996.[85]

The introduction of CDA led to fears that it would create perverse incentives for intermediaries against policing the very content that was attempted to being eliminated and they would allow it to exist on their servers, so that they could avoid being considered a publisher and therefore, unworthy of certain legal protections.[86]

For several years, the competent authority on ISP liability in the US was held by Cubby[87], however the decision of Stratton Oakmont, Inc. v. Prodigy Services[88]changed this. The partial summary judgement held that Prodigy as a publisher and *'whether Prodigy had ever received notice of the allegedly defamatory postings would be a secondary matter'*. In his opinion, Judge Ain argued:

> *"[f]or the record, the fear that this Court's finding of publisher status for Prodigy will compel all computer networks to abdicate control [of] their bulletin boards, incorrectly presumes that*

[83] EFF, Copyright: Digital Millennium Copyright Act, See: https://ilt.eff.org/index.php/Copyright:_Digital_Millennium_Copyright_Act

[84] Communications Decency Act 1996, 47 U.S.C. § 230(c). See:http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm

[85] EFF, CDA a legislative history, See: https://www.eff.org/issues/cda230/legislative-history

[86] Bernstein Solveig, 'Beyond The Communications Decency Act: Constitutional Lessons Of The Internet', Cato Policy Analysis No. 262, November 4, 1996 See: http://www.cato.org/pubs/pas/pa-262.html

[87] *Cubby*, CompuServe argued that it was a distributor and not a publisher and therefore could not be liable for the content because it did not know and had no reason to know about the statements in question. See Cubby, Inc. v. CompuServe Inc. 776 F.Supp. 135 (S.D.N.Y. 1991), Internet Library of Law and Court Decisions, available at: http://www.internetlibrary.com/cases/lib_case69.cfm.

[88] Stratton Oakmont, Inc. et al. v. Prodigy Services Company, et al 1995 N.Y. Misc. Lexis 229, (N.Y. Sup. Ct. Nassau Co., 1995) motion for renewal denied 1995 WL 805178 (Dec. 11, 1995). See: http://www.internetlibrary.com/cases/lib_case80.cfm

the market will refuse to compensate a network for its increased control and the resulting increased exposure." [89]

Stratton Oakmont itself doubted the wisdom of construing ISPs as publishers of third party content and dropped their claim choosing not to contest Prodigy's motion to dismiss.[90]

Originally intended to compete with CDA, Section 230 was introduced as the Online Family Empowerment Amendment or the Cox/Wyden Amendment[91]. Its dual purpose was to overrule Stratton Oakmont and to encourage private efforts to cope with online indecency[92] to remove the disincentives against policing and removing unlawful content. It stated intermediaries may be held liable for third party content only if it violates federal criminal law, intellectual property law, or electronic communications privacy law as well as prevented states from enlarging intermediary liability beyond these federal laws as it preempts all 'inconsistent' state law. Importantly, while Section 230 restricts the civil liability of intermediaries and does protect intermediaries against state criminal legal claims while applicable to nearly all claims that are not IP, it does not protect against federal criminal legal claims.

The CDA was quickly struck down as unconstitutional, though Section 230 survived and has since, been uniformly held to create absolute immunity from liability for anyone who is not the author of the disputed content, even after they are made aware of the illegality of the posted material and even if they fail or refuse to remove it. The section reads: *"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."*

Further, Section 230 contains a provision that protects intermediaries from liability when they voluntarily takedown objectionable and harmful content. The section provides: *"no provider or user...shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected..."*. [93]

The statute also contains a policy statement from the US government that provides safe harbour at §230(B)(4) for any action taken to: *"encourage the development of technologies that*

---

[89] *Ibid.*

[90] Stratton Oakmont v. Prodigy, Digital Media Law Project, May 1995 See: http://www.dmlp.org/threats/stratton-oakmont-v-prodigy

[91] 141 Cong. Rec. 22,044 (1995) See: http://www.yorku.ca/phall/HOME/ACT/950731.html

[92] Section 230 Communication Decency Act, 1996; http://www.law.cornell.edu/uscode/text/47/230

[93] USC Code 230 C Subrule (c) Protection for "Good Samaritan" blocking and screening of offensive material
(2) Civil liability No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected;

maximize user control over what information is received by individuals...to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[94]

Both these provisions promote intermediaries developing community guidelines and voluntary and 'good faith' content removal procedures and technologies for restricting objectionable and harmful content. While not required under the statute, such self regulatory practices and provisions may be interpreted broadly, and can lead to private censorship without due process and accountability which may have an unintended impact on freedom of expression and privacy.

3.6.3 India

The Indian liability regime is partially derived from EU's horizontal framework. The key legislation defining the liability regime for online intermediaries in India is the Information Technology Act (as amended in 2008)[95] and secondary legislation, in particular the 2011 Information Technology (Intermediary Guidelines) Rules[96] also contain provisions to guide the conduct of online intermediaries. The Information Technology Act does not cover the offences related to copyright and for those offences the key legislation is the Copyright Act, 1957. The NTD procedure for copyright related infringements is provided by Rule 75 of the Copyright Rules of 2013.[97]

The IT Act was enacted in 2000 seeking to bring e-commerce and e-government interactions in harmonization with Model Law on Electronic Signatures adopted by United Nations Commission on International Trade Law (UNCITRAL)[98]. It was framed with a threefold objective of firstly providing legal recognition to electronic transactions, secondly, to facilitate the electronic filing of documents with government agencies, and thirdly to amend certain Acts, inter alia, the Indian Penal Code, 1860[99], Indian Evidence Act, 1872[100]. The 2000 IT

---

[94] See USC Code 230 C 'Protection for "Good Samaritan" blocking and screening of offensive material'
(2) Civil liability No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

[95] Information Technology Act (Amendment) Act 2008
See:http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

[96] Information Technology (Intermediaries Guidelines) Rules 2011 See:
http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511%281%29.pdf

[97] Rule 75, Copyright Rules of 2013 http://copyright.gov.in/Documents/Copy-Right-Rules-2013.pdf

[98] United Nations Commission on International Trade Law (UNCITRAL)
See:http://www.uncitral.org/uncitral/en/index.html

[99] Indian Penal Code, 1860 See:
http://www.advocatekhoj.com/library/bareacts/indianpenalcode/index.php?Title=Indian%20Penal%20Code,%201860

Act, included a definition for intermediaries and under Section 79[101] set out provisions limiting liability for network service providers. Under Section 79 intermediaries were protected from liability to the extent that they had no actual knowledge of the offence and if they proved that they had exercised due diligence towards preventing and restricting the unlawful content.[102] The vaguely worded provisions were considered harsh on intermediaries, as they could be held liable if it was proven that they had constructive knowledge or even if they lacked sufficient measures to prevent the offence. Further the provisions shifted the burden of proof on the intermediaries placing an impractical and costly[103] obligation on intermediaries to monitor all traffic and content. Following the criticism of the draconian provisions of the Act and pursuant to the furore resulting from the arrest of the CEO of an online platform for UGC[104], the 2000 Act was amended in 2008.

IT (Amendment) Act 2008 was enacted on 27th October 2009 along with sub-legislation applicable to the liability of intermediaries, in particular, Rules pertaining to Section 69 (Procedure and Safeguards for Interception, Monitoring and Decryption of Information)[105], Section 69A (Procedure and Safeguards for Blocking for Access of Information by Public)[106], Section 69B (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information).[107] The revised provisions under Section 79 established legislation limiting intermediary liability in India and creating a conditional safe harbour regime. Subsequently, on the 11th of April 2011, the Government of India notified the Information Technology (Intermediaries Guidelines) Rules 2011 establishing a 'notice and takedown' procedure for intermediaries under the conditional liability regime of the IT Act[108].

The provisions under the 2008 Amended IT Act and the 2011 Rules together impose conditional safe harbour liability for online intermediaries for all types of legal claims except

---

[100] Indian Evidence Act, 1872 See: http://www.advocatekhoj.com/library/bareacts/indianevidence/index.php?Title=Indian%20Evidence%20Act,%201872

[101] Section 79, *supra note 77*

[102] Section 79, IT Act 2000 See: http://cis-india.org/internet-governance/resources/section-79-information-technology-act

[103] Global Network Initiative, (2014), Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose. See: https://globalnetworkinitiative.org//sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf

[104] Avnish Bajaj vs State, (2005) 3 CompLJ 364 Del, on 29 May, 2008 See: http://indiankanoon.org/doc/309722/

[105] Section 69 *supra note 77*

[106] Section 69A and 69B *supra note 77*

[107] Press Information Bureau, Government of India, 2009 See: http://pib.nic.in/newsite/erelease.aspx?relid=53617

[108] Rules 4 and 5, Intermediaries' Guidelines Rules 2011 supra note 78

those related to Intellectual Property and Copyright. An amendment was introduced in 2012 which brought copyright related offences under the purview of the Copyright Act 1957. The safe harbour provisions are provided for under section 52(1)(b) and (c) of the Copyright (Amendment) Act 2012.

Section 79 of the IT Act introduces the concept of 'notice and takedown' provision. Provision 3(b)[109] under Section 79 renders an intermediary liable, in case upon receiving actual knowledge or upon receiving a notice from a government agency, the intermediary fails to expeditiously remove or disable access to the unlawful material without vitiating the evidence in any manner. Under the 2000 Act, Section 79 placed the burden of proof on network service providers holding them liable for third party content when either they failed to prove that the offence was committed without their knowledge or if proven that that they had not exercised due diligence to prevent the commission of such offence or contravention. The amended Section 79 is a change in the positive direction, as it seeks to make only the actual violators of the law liable for the offences committed.

The Amended section states that the intermediary shall be liable and loses protection of the act if (a) it initiates the transmission; (b) selects the receiver of the transmission; and (c) selects or modifies the information. The first two conditions are necessary to be classified as a 'true intermediary'. The third condition is vague and maybe too broad in its application. The section also provides that the intermediary shall be liable if they have conspired or abetted or induced, whether by threats or promise or otherwise in the commission of the unlawful act Section 79(3)(a). However, it is pertinent to note that the onus to prove conspiracy, which may prove to be difficult has now shifted on the complainant.

The immunity provided to intermediaries, under Section 79, is however, limited by Section 72A[110] which can hold intermediaries liable for disclosure of personal information in breach of a lawful contract. This provision introduced under IT Amendment Act, 2008, is aimed at protection of privacy and personal information of a person. Under Section 72A, intermediaries could still be held liable for disclosure of personal information of any person where such disclosure is without consent, and is with the intent to cause wrongful loss or wrongful gain or in breach of a lawful contract. The punishment for such disclosure is imprisonment extending upto three years or fine extending to five lakh rupees or both. For the

[109] Section 79 IT (Amendment) Act (3) (b): *"upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."*

[110] Section 72 A IT (Amendment) Act (2008). Section 72 of the IT Act provides for penalty for breach of confidentiality and privacy. The Section provides that any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to INR 100,000, or with both.

purpose of this study we will not be covering Section 72A in detail, since it relates liability to the intermediary not for third party content but for disclosing personal information of users. The scope of this study is limited to understanding the regulation of intermediaries in relation to third party content only.

It is important to note that the provisions under Section 69A (blocking public access of any information) grant powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". The provision though outside of the liability regime enacted through Section 79, places liability on intermediaries to block unlawful third party content or information that is being generated, transmitted, received, stored or hosted by the intermediaries. Section 69A has been inserted in the IT Act by the amendments in 2008 and gives power to Central government or any authorized officer to direct any agency or intermediary(for reasons recorded in writing) to block websites in special circumstances as applicable in Section 69.

Under this Section the grounds on which such blocking is possible are quite wide. In this respect, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009[111] were passed vide GSR 781(E) dated 27 Oct 2009, whereby websites promoting hate content, slander, defamation, gambling, racism,violence and terrorism, pornography, violent sex can reasonably be blocked. The 2009 Rules also allow the blocking of websites by a court order and sets in place a review committee to review the decision to block websites. The intermediary that fails to extend cooperation in this respect is punishable with a term which may extend to 7 yrs and or an imposition of fine.

There are two key aspects of both these provisions that must be noted given our two-pillared approach to understanding liability.

a) Section 79 is an exemption provision that qualifies the intermediary for conditional immunity, as long as they fulfil the conditions of the section.

b) Section 69A does not contribute to immunity for the intermediary rather places additional obligations on the intermediary and as the judgement notes. The provision though outside of the conditional immunity liability regime enacted through Section 79 contributes to the restriction of access to, or removing content online by placing liability on intermediaries to block unlawful third party content or information and therefore, restriction requests must fall within the contours outlined in Article 19(2) and include principles of natural justice and elements of due process. For the purpose of this study we will not be covering Section 69 and applicable rules in detail, since it is not limited to liability of the intermediary for third party content but also broader content restriction and for disclosure requirements. The scope of this

[111] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 See: http://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009

study is limited to understanding the regulation of intermediaries in relation to third party content only.

3.6.4 Canada

The most nascent liability regime being covered in this study is the liability regime in Canada with effect from January 2015, defined under the Copyright Modernization Act[112] (CMA). The Canadian liability regime has been shaped by five cases that sought guidance on a host of copyright matters that were largely undecided by law ranging from the fundamental theories underlying copyright, to establishing fair dealing or limits to when copyright may be claimed, to the applicability of copyright in cyberspace.[113] The genesis of distinguishing liability based on the function of the intermediary goes back to 1995, when the Society of Composers, Authors and Music Publishers of Canada (SOCAN) applied to the Copyright Board of Canada for the approval of a new royalty tariff "Tariff 22" to cover copyrighted music transmitted over the Internet e.g., music played on a Web page or music streamed over the Internet, either on demand or via Internet radio stations. SOCAN argued[114] that all parties involved in the transmission of online music, including Internet service providers, bear responsibility for paying an appropriate royalty. Canadian Association of Internet Providers (CAIP) countered that they are mere intermediaries and should not be liable for the content transmitted via their servers. In 2004 the Supreme Court of Canada interpreted Section 2.4(1)(b) of the 1985 Copyright Act known as the "common carrier exemption" to deny claimants royalties for copyrighted material transferred over the internet. The Court held that ISPs are not liable as long as they are content neutral and act as 'conduit' for information. Under this interpretation ISPs are considered to have not communicated the content at all, as long as they can establish that they have been neutral with regard to the content being communicated. This interpretation has also led to intermediaries receiving immunity from defamation liability[115].

Section 31.1 under the CMA is a codification of the holdings from SOCAN v CAIP[116] that expands the exemption granted by Section 2.4(1)(4) of the 1985 Copyright Act.[117] Section 31.1(1) states that ISPs, provided that they are content neutral, cannot be held liable by

---

[112] Copyright Modernization Act 2012, c. 20 Assented to 2012-06-29 See: http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/FullText.html

[113] The Copyright Pentalogy, How the Supreme Court of Canada shook up Copyright See: http://www.press.uottawa.ca/sites/default/files/9780776620848.pdf

[114] Canada: Copyright Law and the Internet - The Tariff 22 Case. See: http://www.mondaq.com/canada/x/27539/IT+Internet/Copyright+Law+and+the+Internet+The+Tariff+22+Case

[115] Para 89 Copyright Modernization Act supra note 93

[116] Supreme Court of Canada, Society of Composers, Authors and Music Publishers of Canada (SOCAN) v Canadian Assn. of Internet Providers (CAIP), 2004 SCC 45, June 30, 2004. See: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2159/index.do

[117] Copyright Act 1985, See: http://cyberlaw.stanford.edu/page/wilmap-canada

providing any means for Internet access. Further, Sections 41.25-41.27[118] under the CMA enact the NTN procedures that have been in place between ISPs and the music and cable industry since 2000 as a voluntary standard adopted to deal with copyright infringement.

Under the NTN regime, a copyright holder can report an infringement by sending a written notice to the ISP, who upon receiving the notice must promptly forward it to the accused subscriber. Further, ISPs are required to maintain record of the user who owns the electronic location at which the alleged copyright infringement occurred for up to six months and if the ISP fails to carry out its obligations it is liable for statutory damages ranging from $5,000 to $10,000.

An exception has been provided to information location tools by limiting remedies against them to injunctions, as long as they are content neutral or, if they are not guilty of '*enabling*' infringement. The provision for enabling copyright infringement under Section 27 (2.3) introduces a new basis for secondary liability for ISPs, if it is determined, that the service is primarily intended for enabling copyright infringement.[119]

3.6.5 South Korea

South Korea has a complex liability regime where regulation of intermediaries is framed around several issues or claims. In South Korea, Article 102(3) of the Copyright Act deals with exempting intermediaries from the obligation of monitoring content. In South Korea the notice and takedown provision similar to that of DMCA is provided for under Article 103 of the Copyright Act. However, beginning from October 2014, online service providers have to adopt technical measures to prevent circulation of obscene material under Article 22-3, TBA. Any service provider in violation of Article 22-3 shall be punished with a civil fine not exceeding twenty million and may have its business registration withdrawn. Similarly, service providers have to take steps to detect child pornography under Article 17, Act on the Protection of Children and Juveniles against Sexual Abuse else they shall be punished by imprisonment with prison labor for not more than three years or by a fine not exceeding twenty million. Article 20 and 20-2, under the Act on Consumer Protection in Electronic Commerce makes the mail order brokers (i.e. online marketplaces) jointly liable in case the seller causes financial damage to the customer. Article 44-2, ICNA requires that the service provider shall immediately delete the information or temporarily block it for up to 30 days as

[118] Section 41.25 Notice of claimed infringement, Section 41.26 Obligations related to notice, Damages related to notices, Regulations —change of amounts, Section 41.27 Injunctive relief only—providers of information location tools. See: http://laws-lois.justice.gc.ca/PDF/2012_20.pdf

[119] Section 27 of the Act is amended by adding the following after subsection (2.3) Infringement —provision of services "It is an infringement of copyright for a person, by means of the Internet or another digital network, to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service.

soon as someone informs them of the alleged infringement. Although Article 44-2 is supposed to be a NTD procedure that creates safe harbor for intermediaries from all kinds of right infringing information (including defamatory content), the wording of the Article is arbitrary. Intermediaries therefore interpret it as a mandatory takedown obligation even if it does not have any penal provision. Paragraph 6 of the Article provides for conditional immunity, which is finally determined by the courts. Therefore, intermediaries are incentivized toward taking down the contents due to the uncertainty it poses. Article 44-5, ICNA is a safe harbour condition that exempts defamation related liability.

In the Constitutional Court decision of 24-1(B) KCCR 578, 2010, it was held that Article 44-2 of ICNA does not infringe upon the freedom of expression which is guaranteed under Article 21 of the Constitution as this is in the public interest, even if it implies that lawful information is taken down. Aside from legislations, Korean Supreme Court has developed an intermediary liability rule of its own, either imposing joint liability on intermediaries as abettors of illegal activity or recognizing "actual knowledge" element broadly. It rarely accepts intermediaries' safe harbor defense under ICNA or the Copyright Act. In a Supreme Court decision, service providers were exempted from liability by the court for allowing subscribers to post copyright infringing materials and enabling the materials to be searched on their portals. According to the decision, service providers are only liable when:

(1) illegality of the copyright infringing material is clear;

(2) the OSP either received a notice from the right holder or was clearly aware of the infringement; and

(3) it is technically and financially possible to control the material.

One of the most criticised decisions of the Supreme Court related to intermediary liability for defamatory content held web portal sites Naver, Daum, SK Communications, and Yahoo Korea liable for the defamation of the plaintiff against whom it had been alleged that he had caused his girlfriend to commit suicide. Barring special circumstances the court held that the intermediary shall be liable for illegal contents to the same extent as a news agency , that is when

(1) the illegality of the content is clear;

(2) the provider was aware of the content; and

(3) it is technically and financially possible to control the contents.

Further the court stipulated that apart from taking down such content immediately, the intermediary also has a duty to block similar postings in the future. The implication of this ruling is that intermediaries will be held absolutely liable for a posting as long as it is

established that it is "clearly" defamatory or if "it was apparently clear that the provider could have been aware of that content", even if the victim did not notify the intermediary of the existence of the content.

3.6.6 Chile

In Chile, the liability regime mostly derives from the Intellectual Property Chapter of the Chile-USA FTA which has been in force since 2004. The Chile-USA FTA strongly follows the DMCA model. The key legislation is Law No. 20.435, enacted on May 04, 2010, which amended Intellectual Property Law. It establishes a new exceptions and limitations framework and implements the Chile-USA FTA regarding intermediary liability, while leaving out implementation of TPM rules. The law includes a definition for intermediaries, and limits liability for network providers, caching providers, and hosting providers and search engines. In the first case, safe harbour is granted if the service providers are not interfering with the content, its originator or its destination. For those service providers who may be processing or interfering with the transmission of content, the common rule is removal of content expeditiously when notified of a court order. Liability is asserted when service providers fail to remove or block the contents, after being dutifully notified of the court order. The US-Chile FTA requires "actual knowledge" as a condition for liability, which was implemented as a court order. Other duties for service providers include identifying the person who will receive the notices and forwarding notices to infringing users within 5 days after receiving them from rights-holders.

3.7 Informal or voluntary measures for enforcing liability

Beyond the provisions contained in statutes, governments also explore technical solutions usually involving the use of filtering software to detect and block alleged unlawful content. This approach, in which the government acts as a broker, is particularly prevalent across UK and USA. For example, in UK under the DEA, ISPs are obliged to take technical measures to limit, suspend or terminate Internet services of relevant subscribers. In exchange for conditional immunity, governments have encouraged intermediaries to explore common, usually 'technical', solutions with various interest groups as a way of dealing with complaints relating to, for example, copyright infringement or the protection of children[120].

This is usually done in the form of "*memoranda of understanding*" or "*best practice codes*". Such codes are encouraged at a global level and an example of this is the Organization for Economic Cooperation and Development (OECD), promulgating a set of principles for Internet policy making in 2011 that encourages member countries to "foster voluntarily developed codes of

[120] Akdeniz, Yaman "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach," in Edwards, L and Waelde, C eds, *Law and the Internet: Regulating Cyberspace*, Hart Publishing, 1997, pp 223-241. See: http://www.cyber-rights.org/reports/governan.htm

conduct" within the private sector to curb illegal behaviors online.[121] Although these procedures provide an expedient and cheap mechanism for addressing alleged wrongdoing online, in reality, their use has a very high cost for the right to freedom of expression.

3.8 Definition and types of intermediaries

Defining which platforms and services constitute intermediaries is critical to developing a balanced regulatory framework for liability. Any definition of an intermediary should account for the various roles and functions that intermediaries perform in relation to unlawful content. It must also note, the different categories of platforms and services being clustered under the definition. This is an important consideration, given that intermediaries serve multiple functions in relation to content, for example a platform may transmit and host third party content and the process of categorization is often, not clear cut.

Further, online intermediaries increasingly employ automated agents such as applications rather than human actors when handling third party content[122]. Search engines are an example of this as they perform as services which offer the user a spectrum of hyperlinks, characterized by the search parameters determined by the user. Based on automatic referencing to desired content could lead to the conclusion that they resemble a technical tool, however, it has to be taken into account that search engines can concentrate on searching specific contents like pictures, music or other digital content.[123] In contrast, hyperlinks are selected consciously which implies that actual knowledge of the content is a prerequisite, even though this does not imply that this would lead to knowledge of changes made in content after the hyperlink has been set. Finally, there are hybrid forms between search engines and hyperlinks, like web sites containing hyperlinks generated by a search engine and results are published to a large community.[124]

More importantly, intermediaries may perform simultaneous and competing roles in relation to producing, disseminating and as end users of content. Another critical distinction to bear in mind is that online service providers may also deliver their own content and definitions must evolve bearing this distinction between 'pure' intermediaries in an intermediation role between

---

[121] OECD, OECD Council Recommendation on Principles For Internet Policymaking 4, 7 (2011) ("These codes would be developed by voluntary participants in a multi-stakeholder process . . . [and] should encourage and facilitate voluntary cooperative efforts by the private sector to . . . address illegal activity . . . taking place over the Internet.").

[122] Perset Karine, 'The Economic and Social Role of Internet Intermediaries', OECD, (April 2010) See: http://www.oecd.org/internet/ieconomy/44949023.pdf

[123] Thibault Verbiest, ULYS Prof. Dr. Gerald Spindler, Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia-and Telecommunication Law University of Göttingen, Giovanni Maria Riccio, University of Salerno Aurélie Van der Perre, researcher at the CRID Under the direction of the Professor Montero University of Namur (FUNDP), 'Study on the liability of Internet Intermediaries', November 12th, 2007, See: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

[124] Ibid 141

third parties and those intermediaries that give access to, host, transmit or index content or services that they themselves originate.[125]

Given the complexity of functions and roles that intermediaries serve, it is not surprising that definition of intermediaries varies widely in its interpretation and application across jurisdictions and regimes. According to the OECD[126], online intermediaries "bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet based services to third parties."

Different types of Internet intermediaries may have different legal responsibilities under the various national or supranational regimes. Both the DMCA and the ECD divide service providers into useful categories by function. The most common categories are mere conduits (or communications or access providers), hosts, providers of caching services, and search engines (or information location tools) or other linking intermediaries.[127]

3.8.1 India

In India, under the 2000 IT Act[128], "intermediary" was defined as any person, who on behalf of another person, receives, stores or transmits messages or provides any service with respect to that message. However, the IT (Amendment) Act[129] clarified the definition "intermediary" by specifically including the telecom services providers, network providers, internet service providers, web-hosting service providers in the definition of intermediaries thereby removing any doubts. Furthermore, search engines, online payment sites, online-auction sites, online marketplaces and cyber cafés are also included in the definition of the intermediary. However, different classes of intermediaries are not clearly defined in the IT Act or the Rules, and there is no parallel legislation in the world which provides immunity to such a wide range of intermediaries however fails to distinguish them basis their class and functions.

The NTD procedure for copyright related offences is provided under Rule 75 of the Copyright Rules of 2013 which also states the scope of exemption available to different types of intermediaries. Carrying forward the language of Sections 52(1) (b) and 52(1)(c), the

[125] I*bid 120*

[126] *Ibid. 120*

[127] The role of internet intermediaries in advancing public policy objectives, Forging partnerships for advancing policy objectives for the Internet economy, Part II See: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP%282010%2911/FINAL&docLanguage=En

[128] IT Act 2000 Section 2(w)
http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf

[129] IT Act 2008 Section 2(w)
http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

exemption to liability is made available for intermediaries who facilitate, "transient or incidental storage of work for providing electronic links, access or integration."

As we have highlighted earlier it is important to distinguish intermediaries based on their role in relation to the alleged illegal content, which could be different depending on the nature of service they are providing. Further, the Copyright Act does not define terms such as "transient", or "incidental" and this may lead to different legal interpretation which may fall outside of the protection granted. Vague definitions open the door to litigation to determine if intermediaries qualify for the safe harbour which is costly.

3.8.2 United Kingdom

Under the ECD, Articles 12-15 introduce liability of online intermediaries and the regime effects ISPs and information society service providers (ISSPs) or, intermediary service providers.[130] The broad definition of an intermediary service provider under the ECD liability regime covers not only the traditional ISP sector, but also a much wider range of actors involved in selling goods or services online.[131] For example, it covers e-commerce sites such as Amazon and eBay, platforms offering online information or search tools that may be for revenue or not for revenue such as Google, BBC News website, and "pure" telecommunications, cable and mobile communications companies offering network access services.[132]

The ECD also notes that even if a service is free to the recipient it falls within the scope of the directive as long as it broadly forms part of an economic activity. This is an important consideration given that, present revenue models where intermediaries give away major product or service for free such as search engines generating revenue laterally from associated advertising. The definition of an intermediary under the ECD is interpreted widely to apply to a host of online activities and platforms. Though the scope has been limited by excluding certain activities from its remit such as gambling, taxation, competition law, and activities of notaries.[133] Data protection regulation and liability for privacy is also excluded from the ECD regime.

The ECD Regulations 2002, follow the same broad definition for intermediaries. The Regulations refer to an *"information society service"* that is defined as: *"any service normally provided for remuneration at a distance, by means of electronic equipment for the processing*

[130] Section 4 Liability of intermediary service providers Article 12-14. See: http://www.oecd.org/internet/ieconomy/44949023.pdf

[131] Lilian Edwards and Charlotte Waelde, 'Online Intermediaries and Liability for Copyright Infringement', See: file:///home/jyoti/Desktop/SSRN-id1159640.pdf

[132] Ibid 128

[133] Article 1, sub rule 5. See: http://www.columbia.edu/~mr2651/ecommerce3/1st/Statutes/ElectronicCommerceDirective.pdf

(including digital compression) and storage of data, at the individual request of a recipient of the service".[134]

The UK Department of Trade and Investment (DTI) Guidance on the Regulation states that: *"The requirement for an information society service to be 'normally provided for remuneration' does not restrict its scope to services giving rise to buying and selling online. It also covers services, insofar as they represent an economic activity, that are not directly remunerated by those who receive them, such as those offering online information or commercial communications (e.g. adverts) or providing tools allowing for search, access and retrieval of data."*[135]

The ECD address the civil and criminal liabilities of ISPs acting as intermediaries, distinguishing between them as mere conduits, caching providers and hosting providers.[136] The directive establishes liability based on the function of the intermediary as ISPs and any other entities whose role it is to route and transmit Internet communications. Intermediaries are exempted from liability as long as they do not initiate the transmission, select the recipients, or select or modify the selected content.

Information location tools were not included in the initial definition of intermediaries. Subsequently, in 2010 Court of Justice of the European Union (CJEU) was asked in *Google France SARL, Google v Louis Vuitton Malletier SA and others*[137] whether Google search fell within the definition of an *'information society service'*. CJEU found that: *"An internet referencing service constitutes an information society service consisting in the storage of information supplied by the advertiser"*. The court also emphasised that for a service to fall within the definition of an information society service there must be evidence *"that that service features all of the elements of that definition"*.

In 2009 the UK High Court asked CJEU to provide a preliminary ruling in *L'Oreal v eBay* (2011)[138], in considering eBay's potential liability for selling L'Oreal products online without consent. In its ruling the court accepted that eBay as the operator of an online marketplace was an information society service. In another preliminary ruling,[139] CJEU clarified that if the

---

[134] Electronic Commerce (EC Directive) Regulations 2002 See: http://www.legislation.gov.uk/uksi/2002/2013/pdfs/uksi_20022013_en.pdf

[135] DTI Guide for Business To the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) http://webarchive.nationalarchives.gov.uk/20121212135622/http://www.bis.gov.uk/files/file14635.pdf

[136] Article 1.2 of Directive 98/34/E Definition of information society service

[137] Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08). See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62008CJ0236

[138] L'Oreal v eBay (2011) http://curia.europa.eu/juris/document/document.jsf?docid=107261&doclang=en

[139] Nils Svensson and Others v Retriever Sverige AB, See: http://curia.europa.eu/juris/document/document.jsf?docid=147847&doclang=EN

rights holder makes a work available without restrictions on the Internet, any linking to that content would not create a new public and is therefore authorized.[140]

Online intermediaries in UK also sought defense against liability for defamation, relying on the defense laid out in Section 1 of the Defamation Act. Under UK defamation law, website hosts were not liable for defamatory user generated content provided as long as they did not in some way participate in its initial publication, for instance by vetting or editing it before publication. Thereafter, if a complaint was made, the website host had the choice to take down the material, in which case it would not be liable; or leave the material on the website, in which case it would assume responsibility and liability for it. The Act defines the term publisher in Section 1(2) as: *"a commercial publisher, that is, a person whose business is issuing material to the public, or a section of the public, who issues material containing the statement in the course of that business."*[141]

The 'intermediary' defence was outlined by the overlapping provisions of the Defamation Act, the Regulations, and as developed by a body of case law starting with the landmark case of Godfrey v Demon[142]. This was contradicted in the 2012 ruling in Tamiz vs Google[143] where Justice Eady ruled: *"It is no doubt often true that the owner of a wall which has been festooned, overnight, with defamatory graffiti could acquire scaffolding and have it all deleted with whitewash. That is not necessarily to say, however that the unfortunate owner must, unless and until this has been accomplished, be classified as a publisher."* [144]

The decision was taken to the Court of Appeal, which agreed that, Google should not be considered a publisher, however, went on to adopt a notice board analogy to determine Google's role as a publisher after notification: *"The provision of a platform for the blogs is equivalent to the provision of a notice board; and Google Inc goes further than this by providing tools to help a blogger design the layout of his part of the notice board and by providing a service that enables a blogger to display advertisements alongside the notices on his part of the notice board. Most importantly, it makes the notice board available to bloggers on terms of its own choice and it can readily remove or block access to any notice that does not comply with those terms."*[145]

Crucially, the Court of Appeal stated that if Google allows defamatory material to remain on a blog after it has been notified of the presence of that material, it could be considered to be a

---

[140] Chris Marchich, CJEU Judgment Will Help Rights Holders Create New Services for Consumers and Protect Their Content Online. See: http://blog.mpaa.org/BlogOS/author/Chris-Marcich.aspx

[141] Ibid. 131

[142] Godfrey v Demon Internet Ltd Reference [1999] EWHC QB 240; [1999] 4 All ER 342 See: http://www.5rb.com/case/godfrey-v-demon-internet-ltd/

[143] Tamiz v Google 2013) EWCA Civ 68 See: http://www.fieldfisher.com/publications/2013/02/normality-restored-website-hosts-may-again-be-liable-for-defamatory-user-generated-content#sthash.2UMv9uPV.dpuf

[144] Para 16 Tamiz v Google [2013] EWCA Civ 68. See: http://www.5rb.com/wp-content/uploads/2013/02/Tamiz-v-Google-CA.pdf

[145] Para 33 *Ibid.*

publisher and held liable for the continued presence of that material on the blog. However, the court ruled in favour of Google on the basis that it is unlikely that a significant number of readers had accessed the comments concluding *"the game would not be worth the candle"*.[146]

In UK, the DTI has recently considered whether to explicitly extend the liability limitations in Articles 12 to 14 ECD to hyperlinking services, location tool services and content aggregation services, but has concluded that there is currently no substantial evidence to support the case for an extension.[147] However, it also noted in the DTI report that the legal situation as regards the need for an exemption on liability is less clear in some other member states such as France and Germany.[148]

3.8.3 United States of America

In the United States, under a vertical framework separate liability regimes exist for copyright claims under Section 512 of the DMCA, trademark claims under Section 32(2) of the Lanham Act[149] and non-intellectual property claims under Section 230 of the CDA 1996[150]. The copyright regime set out under DMCA recognises the following different classes of intermediaries based on the kinds of actions that they perform:

(1) Transitory digital communications networks – transmitting, routing or providing connections

(2) System caching – intermediate and temporary storage

(3) Information residing on systems or networks at direction of users (hosting) storage

(4) Information location tools – referring or linking[151]

DMCA grants immunity to intermediaries contingent to certain due diligence requirements and while certain requirements are common for all types of intermediaries, others exclude transitory digital communications networks. DMCA makes this distinction since this class of intermediary involved in transmitting, routing and provision of connection plays a passive role by acting as mere carriers of data provided by third party.

---

[146] Para 28 *Ibid.*

[147] DTI consultation on extending liability protection to hyperlinks, search engines and aggregation services (2005), Government responses and summaries of responses, December 2006. See: http://webarchive.nationalarchives.gov.uk/20070603164510/http://www.dti.gov.uk/files/file35905.pdf

[148] Verbeist Thibault, Dr Gerald Spindler, Giovanni Riccio et al. 'Study on the Liability of Internet Intermediaries', November 12, 2007, See: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

[149] The Lanham Act, 15 U.S.C. §§ 1051 *et seq. See: http://www.law.cornell.edu/uscode/text/15/chapter-22*

[150] *Supra note no 69*

[151] See DMCA Section 512, [a, b, c] See:http://www.copyright.gov/title17/92chap5.html#512

The conditions disqualifying the intermediary from liability are based on the intermediary not having any control over the data transferred through its network. DMCA also provides exemption for intermediate or transient storage to accommodate the need for transmissions to be broken down in packets and other store and forward techniques.[152] The DMCA creates a conditional safe harbour for functions of transmission and routing ("mere conduit" functions), caching, storing, and "information location tools" including online directories and providing links to third party materials alleged to infringe the copyrights of others.

The CDA unlike the copyright regime of the DMCA, does not differentiate between classes of intermediaries. Following the vertical framework, the CDA deals with non-intellectual property rights related claims and provides flexibility to the intermediaries as they do not inherit liability on editing UGC. It grants legislative immunity from liability for providers and users of an *"interactive computer service"* who publish information provided by others: *"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."*[153]

Section 230 of CDA has been interpreted broadly, including in cases of defamation[154], privacy, fraud[155] or spam[156]. Under the CDA, the term *"interactive computer service"* means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.[157]

3.8.4 Canada

In Canada, Section 2.4(1)(b) of the 1985 Copyright Act known as the "Common Carrier Exemption", states that an intermediary is not liable for copyright infringement by merely providing *"the means of telecommunication necessary"* for others to communicate digital content.[158] It should be noted that this section is only applicable in cases where the intermediary is involved in the communication of copyright materials. The amendments contained under CMA cover both communication and reproduction of those materials,

---

[152] Section 512 DMCA sub rule (4) "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"

[153] *Supra note no. 27*

[154] EFF archive of Defamation: CDA Cases See: https://ilt.eff.org/index.php/Defamation:_CDA_Cases

[155] Goddard v. Google, Inc. See: http://en.wikipedia.org/wiki/Goddard_v._Google,_Inc.

[156] Levine R. John, Spam legal decisions, See: http://jl.ly/Email/spamcases.writeback

[157] I*bid.*

[158] Section 2.4(1)(b) Copyright Act Canada (R.S.C., 1985, c. C-42) See:http://laws-lois.justice.gc.ca/eng/acts/C-42/index.html

specifically, Section 31.1 states that ISPs, provided that they are content neutral, cannot be held liable by providing any means for Internet access. The fact that "any means" for telecommunication is used instead of "the means" necessary for telecommunication, which appears in section 2.4(1)(b), signifies that this provision is intended to cover a wider range of intermediaries that provide access to third party content such as bloggers, video and social networking websites.[159]

The protection granted by section 31.1 also applies to hosting services under section 31.1(2) and to caching activities by virtue of section 31.1(3), and both these provisions provide protection to ISPs from copyright infringement as a result of caching or other "incidental" acts that provide more efficient Internet services. Further, under section 31.1(4), ISPs are immune from copyright liability related to hosting, unless they know the content provider has been found by a court to infringe copyright. However the immunity from liability contained under section 31.1 is not available to intermediaries whose primary function is to "enable" copyright infringement. Section 27(2.3) of CMA creates a new basis for ISP liability if the service is primarily intended for enabling copyright infringement.

The conditions of "enabling" remain unclarified and for the courts to determine. CMA also defines "information location tool" as *"any tool that makes it possible to locate information that is available through the Internet or another digital network."* Further, CMA Section 41.27 specifies, that in any proceedings for infringement of copyright, the owner of the copyright is not entitled to any remedy other than an injunction against a provider of an information location tool that is found to have abetted the infringement.[160]

The leading decision on ISP liability, SOCAN v CAIP also known as the 'Tariff 22' case further clarified the definition of an intermediary. The court interpreted the section 2.4(1)(b) of the Copyright Act and found that ISPs are not liable as long as they are "conduit" for information.[161] That is, if an intermediary remains content neutral, they are considered not to have communicated the content at all[162] and for this reason, intermediaries are also immune

---

[159] Centre for Internet and Society, Stanford WILMAP: Canada. See: http://cyberlaw.stanford.edu/page/wilmap-canada

[160] Section 41.27 Injunctive relief only—providers of information location tools CMA 2013 Canada. See: http://laws-lois.justice.gc.ca/PDF/2012_20.pdf

[161] Para 32, Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers, [2004] 2 SCR 427, 2004 SCC 45 (CanLII). The Copyright Board held that "the normal activities of Internet intermediaries not acting as content providers do not constitute "a communication" for the purpose of the Copyright Act and thus do not infringe the exclusive communication rights of copyright owners." See: http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html?searchUrlHash=AAAAAQAdU09DQU4gdi4gQ2FuYWRpYW4gQXNzb2NpYXRpb24AAAAAAQ

[162] Para 111 I*bid.*

from defamation liability[163]. The courts clarified that whether an intermediary is regarded a conduit for information and thus qualifies for immunity will primarily depend on its function. The Court further held that ISPs and other intermediaries, benefit from the exception only if they restrict their activities as a conduit for information and do not engage in acts that relate to content.

As ISPs may play a variety of different roles with respect to transmission of communication online, including acting as a "host server", which may include the storing, making available and transmitting of content by the ISP to end users.The Court concluded that the liability of a host server must be determined in the same manner as the liability for ISPs generally, namely whether the host server steps outside its role as a mere conduit.[164] Where a host server does act outside its conduit role, liability may be imposed regardless of its location.[165] Host servers need not be located in Canada to be found liable, nor does location in Canada result in automatic liability.[166]

In Crookes v Newton[167] the Supreme Court of Canada considered whether a simple reference — like a hyperlink — to defamatory information is the type of act that can constitute publication. Defamation cases in Canada are conditional to the plaintiff proving that the defamatory statement has been 'published'.[168] The court ruled that the act of hyperlinking is passive and does not amount to publishing, unless the hyperlink itself communicates a defamatory meaning in the context.[169] Further the court clarified that to satisfy the publication element, the plaintiff must prove that the intermediary had "knowing involvement in the publication of the relevant words.[170]

3.8.5 South Korea

In South Korea intermediaries are differentiated as mere conduits, hosting, caching and information location tools. Article 102 (1) of the Copyright Act sets out specific conditions necessary for safe harbor for different types of Online Service Providers (OSPs). It classifies OSPs into four classes mere conduits (subparagraph 1), caching (subparagraph 2), hosting (subparagraph 3), and information location tools (subparagraph 4).[171] Article 104 is a unique

[163] Para 89 *Ibid.*
[164] Para 107 *Ibid.*
[165] Para 135 *Ibid.*
[166] Para 106 *Ibid.*
[167] Crookes v. Newton, 2011 SCC 47, [2011] 3 S.C.R. 269. See: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7963/index.do
[168] Brian N. Radnoff & Amy P. Archer, Defamation Law in Canada in an Electronic World, LEXPERT Business of Law (16 October 2014). ttp://www.lexpert.ca/directory/feature-articles/defamation-law-in-canada-in-an-electronic-world-23/
[169] Para 21 *Crookes v. Newton* supra no 139
[170] Para 48 *Crookes v. Newton* supra no 139
[171] Copyright Act, last amended by Act No. 12137, Dec. 30, 2013 (English Version) See: http://cyberlaw.stanford.edu/page/wilmap-south-korea

provision to regulate special types of OSPs which mainly includes P2P and web-hard service providers (cyber lockers).[172] Under the Act on the Consumer Protection in Electronic Commerce, Article 2 subparagraph 4 defines "mail order brokerage" as *"the act of intermediating mail order between both parties to a transaction by allowing the use of a cybermall (referring to a virtual shopping mall established to transact goods, etc. by using computers, etc. and information communications facilities), or by other methods prescribed by Ordinance of the Prime Minister."* For example, Korea's largest online marketplace Gmarket owned by eBay Korea is a mail order broker according to the definition.[173]

3.8.6 Chile

Two legal bodies contain definitions for internet intermediaries in Chile. The first is the General Telecommunications Law, as amended by Law No 20.453, 2010 which establishes. Here, internet providers are defined as *"all natural or legal persons that provide commercial connectivity services between users or its networks and the Internet"*. Under this law, general neutrality rules that is the non-interference with content and transparency regarding network management measures are established for them. The second definition of intermediaries is given by Law No 20.435, as article 5 letter y) of Law No 17.336, that defines a service provider as *"an entity providing transmission, routing or connections for digital online communications, without modification of their content, between or among points specified by the user of material of the user's choosing, or a provider or operator of facilities for online services or network access"*. This closely follows both DMCA and the FTA, but unlike net neutrality law, it is specifically set for legal persons.

3.9 Conclusion

There are a number of common trends across the liability regimes introduced above, and we shall cover these in detail across our evaluations of the categories below. We have identified the two-pillared lens for looking at provisions for liability to understand if they create an immunity based regime for intermediaries or if they are imposing obligations not related to immunity or if countries have adopted a mixed approach. We have also identified if the liability regimes differentiate between intermediaries, an important consideration from the perspective of regulating carriage of communications.

At the outset two features that stand out across regimes and should be noted when developing policy framework for intermediary liability. The first, relates to the legislation and frameworks adopted. As highlighted above, countries may apply several parallel provisions to guide the liability of intermediaries across a wide variety of issues. This may be a result of hauling existing legislation to accommodate the evolving technological landscape and expanding roles of the intermediaries. It may also be that frameworks and standards develop as a way to cope

[172] Ibid. 163 [4]
[173] Ibid 163

with existing legislation, as is the case with Voluntary Copyright Alert Programme being discussed by ISPs in UK[174] and the Copyright Alert System in the USA[175]. Second, implementation of the same framework may vary widely, so for example, EU's horizontal framework implemented into UK law through the 2002 regulations, does not provide immunity from voluntary takedowns.

The vertical framework followed under the DMCA in US, provides immunity from voluntary takedowns while the vertical framework of the Indian liability regime does not. Any approach to regulation of intermediaries must consider why the legislation was enacted and how it is being implemented. This is crucial to our understanding of how norms were developed and how they are evolving or need to evolve with respect to changing technology and regulatory environment.

4 Evaluation of the legal measures adopted

The Principles framework lays out a set of baseline safeguards and best practices related to content restriction online. The first principle states that intermediaries should be shielded from law for third party content and we have attempted to understand the legislative frameworks for each of the jurisdiction included in the study. In the first section of this paper we draw out the provisions that create liability and the procedural approach outlined under the regime. This second part of the paper section evaluates the legal measures adopted across the selected countries to understand if the legislation adequately balances legitimate priorities such as appeal, redress and transparency.

We have organised our analysis around two parameters, first looking at procedures outlined under the regime and comparing them based on criteria that we have developed based on the Manila Principles. The second parameter is organised how intermediaries process user information and what their responsibilities should be under a balanced liability framework.

The second principle states that content must not be restricted without a judicial order, in essence clarifying that liability imposed on intermediaries must be proportionate and correlated to the intermediaries' non-compliance with the court order. The principles also outline the information that should ideally be contained in content restriction orders coming from the courts.

The third principle clarifies that when restriction orders fall outside of those being issued through court orders, there should some basic safeguards incorporated into the notices whether they follow from private requests or are based on the intermediaries' content

[174] Dave Lee, 'Deal to combat piracy in UK with 'alerts' is imminent', BBC, 9 May 2014. See: http://www.bbc.com/news/technology-27330150

[175] Cooke Chris, CMU, 'UK ISPs negotiating voluntary 'strike one' system to combat piracy', May 2014 - See: http://www.completemusicupdate.com/article/uk-isps-negotiating-voluntary-strike-one-system-to-combat-piracy/#sthash.f7zVQoB9.dpuf

restriction policies. These include proof and description of illegal content, Internet identifier of the alleged illegal content and evidence sufficient to document the legal basis of the order and where appropriate an indication of the time period for which content should be restricted.

Some of the criteria that we are considering that relate to this principle two and three including whether knowledge is interpreted as actual or constructive, prescribed persons with locus standi to bring forward notice forward and if there is requirement of the signature of the complainant in the notice. We also look at whether notices are being funneled through the executive or a judicial body. Specifically the criteria we have developed around the third principle includes the time frame for forwarding notice from complainant, prescribed level of proof for takedown, requirement of an intermediary to publish content policy and whether the signature of complainant is included in the order.

The fourth principle stresses the need for restriction orders and practices within liability regimes to comply with the tests of necessity and proportionality. The criteria that we have developed around this principle include consideration of whether a graduated response scheme is in place, the requirement for termination of user account for violations, time frame for removal of contested content, requirement to give a reasoned decision and the requirement to retain removed or restricted information under the regime.

The fifth principle establishes the due process which should be at the heart of any balanced liability framework. It considers issues such as the right to be heard, post facto review, the right to appeal and setting up mechanism to review the decision to restrict and measures to reinstate content that has been wrongfully restricted, including specifying the time period within which content must be put back. Further the principle also touches upon intermediaries' responsibility in relation to user information and we have have dealt with these as a separate parameter in our analysis. We consider the following logging of identification details, of information accessed, sharing user information with private parties through requests or court orders and with law enforcement and or in the interest of national security. We also look at if there are co-operation obligations including providing assistance for interception by government or its agents outlined under the regime.

The sixth and the final principle deals with transparency and accountability which should be built into balanced liability frameworks and we analyse the requirement to publicly disclose data of takedowns or terminations.

4.1 Knowledge and obligation to act

As online service providers generally only have a limited degree of knowledge about the data they transmit or store, the liability allocation between online service providers and the persons who originally put such information online can be problematic. Under most existing liability regimes the intermediary is protected from liability if they take action upon being made aware

of unlawful content. While procedures for dealing with the unlawful content varies across regimes, the precondition for the intermediary taking action is that the intermediary has knowledge of unlawful activity on their networks or platforms.

The assessment of knowledge criteria varies in its implementation and court practice differ across regimes considerably. Some member states require a formal procedure and an official notification by authorities in order to assume actual knowledge of a provider, while others leave it for the courts to determine actual knowledge[176]. At the heart of the issue of knowledge is the conflict of interest that arises from the difficulties of legal analysis of unlawful content on the part of a technical intermediary and liability exemptions that may be dependent on them actively restricting certain content. Another related issue is the question of locus standi or who has the authority to bring the claim forward to the intermediary and if there is a set procedure following the receipt of knowledge to be followed by the intermediary.

4.1.1 United Kingdom

In EU, a distinction based on active and constructive knowledge is made for the knowledge requirement for civil and criminal claims.[177] ECD Regulations carry out near verbatim transposition of *Article 14 ECD* into the national legal system. In UK, intermediaries may be held criminally liable only where they have actual knowledge, whereas civil liability for damages is subject to the lower threshold of constructive knowledge derived from '*awareness of facts or circumstances from which illegal activity or information is apparent*'.[178] Regulation 19 of the ECD Regulations 2002 goes slightly further, protecting an intermediary who does not have *"actual knowledge"* (i.e. is not on notice) or is not aware of facts or circumstances from which it would have been apparent that the information is unlawful (as opposed to merely defamatory).[179]

Caching providers and hosting providers can only benefit from the limited liability regime when they expeditiously remove or disable access to illegal information as soon as they either *"have actual knowledge"* or constructive knowledge.[180] While these concepts are crucial to adequately determine the liability of caching and hosting providers, the ECD does not define what should be considered as *"actual knowledge"* or *"awareness"*. Consequently, it is left to the courts to determine which level of knowledge or awareness is required.

---

[176] In Germany a notice may in principle be given by any person or authority and includes a system of warning. For more details see *supra note no 123*

[177] See Article 18-22 ECD 2000 *supra note no 52*

[178] See Regulation 19 *supra note 56*

[179] Regulation 19 (a)the service provider—(i)does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful

[180] Regulation 18 (b) (5) and Regulation 19(a)(ii) *supra note 56*

The case law across EU has established that the term actual knowledge implies actual human knowledge, as opposed to computer knowledge and negligence and conditional intent were not considered to constitute actual knowledge.[181] The ECD also does not specify a *procedure*, nor clarify the *locus standi* for bringing the unlawful activity to the actual knowledge of the intermediary.[182]

Section 5 of the *Defamation Act 2013*[183] and accompanying *regulations*[184] create a defence for the operators of a website hosting user generated content if the operator can show that it did not post the statement on the website. The regulations specify the threshold for *actual knowledge* on part of the operator under the accompanying regulations by setting down the requirement of a notice for the operator to be held liable. Further, they also specify the *procedure* for the website operator to act after receiving notice of the defamatory statement to in order to claim defence from liability.[185]

Importantly, it should be noted that the defence for operators under section 4.2 of the regulations is defeated if the claimant can show that he or she did not have sufficient information to bring legal proceedings against the person who posted the statement; or that despite being made aware of the statement by a notice of complaint the operator failed to respond to that notice in accordance with the set procedure or if the claimant can show that the operator acted with malice in relation to the posting of the statement.[186] The affected person against whom the defamatory statement has been made has the *locus standi* to bring the notice forward to the intermediary.[187]

The *DEA* establishes a threshold of *actual knowledge* for the ISP to take action limiting liability for the intermediary conditional to the rights holder, having made the ISP aware of the infringing material by way of a CIR.[188] Regulation 3 limits the *locus standi* to copyright owners who have the onus to establish that an infringement of their material is taking place by seeking unauthorised sources including IP address along with date and time stamp. The

[181] 'Study on the liability of Internet Intermediaries', November 12th, 2007 *supra note 123*
[182] *Ibid.*
[183] Section 5, Defamation Act 2013 c. 26. See: http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted
[184] Subrule 2 Notice of complaint: specified information, The Defamation (Operators of Websites) Regulations 2013 No. 3028 See: http://www.legislation.gov.uk/uksi/2013/3028/contents/made
[185] Citation
[186] See (4.2) Legislative Context, Explanatory Memorandum to the Defamation (Operators of websites) Regulations 2013 No. 3028 See: http://www.legislation.gov.uk/uksi/2013/3028/pdfs/uksiem_20133028_en.pdf
[187] *Supra note 151*
[188] Regulation 3 Obligation to notify subscribers of reported infringements Digital Economy Act UK 2010, *supra note 59*

section also lays down a *procedure* for the subsequent action on part of the intermediary once they have received actual knowledge in the form of CIR from the copyright holder.[189]

4.1.2 United States of America

In US the knowledge requirement includes both active and constructive knowledge. The *actual knowledge* requirement is fulfilled by a prescribed form of notice for takedown; and the *constructive knowledge* criteria is fulfilled by determination of the 'red flag' test set under Section 512 of the DMCA, looking into the obviousness of the infringement on being sent a defective notice. The red flag test stems from the language in the statute that states that *"aware of facts or circumstances from which infringing activity is apparent."*[190]

Further the Section 512 of the DMCA sets out a *procedure* for action on part of the intermediary upon receiving both constructive and active knowledge and a service provider need not monitor its service or affirmatively seek facts indicating infringing activity in order to claim this limitation on liability[191]. However, if the service provider becomes aware of a *'red flag'* from which infringing activity is apparent, it will lose the defense against liability if it takes no action. The red flag test has both a subjective and an objective element.[192] In determining whether the service provider was aware of a red flag, the subjective service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a red flag—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances—an objective standard should be used.[193] The Section 512 of DMCA also sets out the *locus standi* for claims as: *"...a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed."*[194]

4.1.3 India

In India, Section 79(3)(b) creates a knowledge requirement standard of "receiving actual knowledge" or being notified by the appropriate Government or its agency for administering takedown. However, Rule (3)(4) of the Intermediary Guidelines prescribes an alternate knowledge requirement standard of *"obtaining knowledge by itself"*; or *"brought to actual*

---

[189] 124A Obligation to notify subscribers of copyright infringement reports, *Ibid.*

[190] Sub rule 3 Elements of a notification, (B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

[191] Or, indeed any other limitation provided by the legislation. See: sub rule (c)(1)(A)(i, ii, iii)

[192] Eric Evans, From the Cluetrain to the Panopticon: ISP Activity Characterization and Control of Internet Communications, 10 Michigan Telecommunications and Technology Law Review 445-499 (2004). See: http://repository.law.umich.edu/mttlr/vol10/iss2/4

[193] *Ibid.*

[194] Sub rule 3 Elements of a notification. Section 512 DMCA See: http://www.copyright.gov/title17/92chap5.html#512

knowledge by an affected person...".[195] It should be noted that the Rules have been notified in exercise of the powers conferred by 87(2)(*zg*) read with 79(2)[196] and therefore, the takedown requirement under 79(3)(b) exists independently of the takedown and knowledge requirement under 79(2).[197]

Further, the Intermediaries Guidelines do nothing to clarify what would amount to "actual knowledge", to indicate in unambiguous terms, which parties would have *sufficient locus* to bring complaints in order to be deemed an "affected person"[198] for the purposes of these provisions or to suggest that there is a *procedure* or timeline for action by the intermediary, such that requirements such as a notice to the author of the content and time for the preparation of a defence by the author and/or the intermediary are accounted for.[199] Importantly, it should be noted that it is also not clear who may constitute an affected person for the purpose of the Rules when the expression relates to cognizable offences such as gambling.[200]

Under Rule 75 of the Copyright Rules, 2013 the intermediary must receive actual knowledge of the copyright infringement in the form of a complaint by the owner of the copyright. The affected person must also file an infringement suit in the competent court against the person responsible for uploading the content.

4.1.4 Canada

In Canada, Section 41.26 sets out a notice and notice procedure which establishes a standard of actual knowledge for the intermediary to be held liable for infringements.[201] In *Carter v B.C. Federation of Foster Parent Association*, the Court of Appeal for British Columbia held the operator of a discussion forum liable for the defamatory remarks posted by its participants based on their failure to remove them within a reasonable time after being notified. The court also clarified that an intermediary cannot seek exemption under the 'innocent disseminator' defence upon receiving notice of offending content.

The court further delved into the issue of whether a statement should be interpreted as per the 'single publication rule' i.e. does a limitation period run once the statement is published online and each subsequent delivery or service is not cause for action or should each subsequent

---

[195] Intermediary Guidelines Rules 2011 *supra note 78*

[196] Intermediary Guidelines Rules 2011 G.C.R. 314 E. *supra note 78*

[197] IT (Amendment) Act 2008 Section 79 *supra note 77*

[198] Uppaluri Ujwala, Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011, Centre for Internet and Society, (16 July 2012) See: http://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules

[199] *Ibid. 165*

[200] Rishabh Dara, appendix 3.1.4.5. supra note 24

[201] 41.25 Obligations related to notice See: http://laws-lois.justice.gc.ca/PDF/2012_20.pdf

publication lead to a distinct cause for action.[202] The court held that: *"If defamatory comments are available in cyberspace to harm the reputation of an individual, it seems appropriate that the individual ought to have a remedy...I do not consider that it would be appropriate for this Court to adopt the American rule over the rule that seems to be generally accepted throughout the Commonwealth; namely, that each publication of a libel gives a fresh cause of action."* [203]

The Canadian regime establishes the copyright owner to have the locus standi to sent forth a notice to the ISP identifying the alleged infringement. However, it should be noted that the requirement of constructive knowledge on part of the intermediary has not been established or tested in the court. Also the legislation does not clarify if where a notice of alleged infringement has been received by an ISP in relation to some subject matter, it is not liable for failure to prevent future infringement in relation to that subject matter."[204] CMA sets out a *procedure* for action on part of the intermediary upon receiving knowledge to forwarding the notice of the infringements to the person making the content available online.

4.1.5 South Korea

Art 44-2(1) and (2), ICNA in South Korea requires every service provider to act immediately upon receiving information about infringement by either deleting the information, blocking it for upto 30 days or any other action that it deems fit.

4.1.6 Chile

Chilean law considers "actual knowledge" the standard for removal of content as a safe harbour requirement. Removal of content for caching providers was established by the USA-Chile FTA as proceeding in the face of "effective notification of claimed infringement", and for hosting providers and search engine, as proceeding when "obtaining actual knowledge of the infringement or becoming aware of facts or circumstances from which the infringement was apparent". These two vaguely different rules were implemented as one procedure, and actual knowledge (mentioned explicitly only regarding hosting providers and search engines) exists "when a competent court of justice, according to procedure established in article 85 Q, has ordered the removal of data or the blocking of access to them and the service provider, having been legally notified of such order, does not comply expeditiously".

Article 85 Q establishes the procedure under which content can be removed. Because the notice is sent through courts, requirements include general obligations for all judicial action, indication of allegedly infringed rights, their entitlement, the form of infringement; indication

[202] Para 14 and Para 18, *Carter v. B.C. Federation of Foster Parent Ass*n., 2005 BCCA 398, August 3, 2005. See: http://www.canlii.org/en/bc/bcca/doc/2005/2005bcca398/2005bcca398.html

[203] As summarized by the Court of Appeal in Carter v. B.C. Federation of Foster Parents Assn., 2005 BCCA 398 at para. 20 and 21 *Ibid.*

[204] Francois Joli-Coeur, Canada's Approach to Intermediary Liability for Copyright Infringement: the Notice and Notice Procedure, Berkeley Tech. L.J. Bolt (March 2, 2014), http://btlj.org/?p=3223.

of the infringing content; and indication of the location of infringing content in the network or systems of the respective provider. The court will decree "without delay" the removal or blocking of infringing contents, to be notified by official document to the service provider. The service provider can require the court to leave without effect the measure, by issuing a request under the same terms than the request for removal.

4.2 Obligation to act

Across some countries the law provides for 'expeditious' action, however, the meaning of the term expeditious and it application may vary in the context of law and across regimes.[205] Using ambiguous terms that are undefined or that do not clarify the time period for action on part of the intermediary in order to claim defense from liability, may lead to confusion in their interpretation under common law. Further, such terms do not adequately represent the time that may required if alleged content is to be removed following due process that ensures the unlawful activity is verified or allowed to be contested including the users' right to be heard.

Differing technical factors may also ascertain the timeframes necessary for removal or restriction of content. Further, depending on the nature of the infringement and the potential damage that the unlawful material may cause the standard for acting expeditiously may or should vary. For example there might be different expectations for timely action on the part of the government or its agencies for intermediaries to restrict content that may incite violence or content, copyrighted images may lead to millions of downloads and may require intermediary to act within few hours and other circumstances may require a more factual determination.

The time concerns get further exaggerated when legal advice is factored in including the availability of resources to determine if the notice complies with set standards within statutes or the means of communicating the notice. The process for restricting content might also contribute to determining what is expeditious action on the part of the intermediary, so an automated system may allow content to be restricted or takedown almost instantaneously whereas a manual system might need more determination and take longer.

Paradoxically, leaving the determination of what constitutes as expeditious to the courts is an expensive and fact intensive procedure, which leaves the intermediary without a proper framework to gauge when their actions are expeditious enough. It should be highlighted that ambiguousness in defining what constitutes expeditious action on part of the intermediary may lead to both over compliance by taking down content without due process. Another side effect of the defense of an intermediary being linked to expeditious removal may be that it may lead to restricting or cutting off access for some users and may open up intermediaries to a host of other claims. A balanced liability regime should provide a definite and reliable framework to gauge whether they are responding properly and satisfying provisions set under

[205] Thibault Verbiest, *supra note 123*

statutes. Therefore, it is necessary to create specific guidelines for evaluating if an intermediary has responded expeditiously.

4.2.1 United States of America

In the US Section 512 of the DMCA states one of the conditions limiting liability of the intermediary is if, "the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement."[206] Even though the DMCA establishes certain safe harbors that protect service providers from liability, and aims to define the threshold requirements for ISPs to qualify for protection under § 512, it does not clearly or adequately explain what constitutes an expeditious response by a service provider in order for the provider to claim defense under the safe harbors of § 512. As a result, the meaning of expeditious remains "open to debate."[207] The function of the term under US case law has been applied as a constructive term, leaving courts to decipher and interpret what is an adequately "expedient" response by a service provider and this has consequently led to lack of uniformity. No court to date has found a service provider liable for a failure to act expeditiously to a takedown notice. It should also be noted that even if it is ascertained that an ISP did not act expeditiously and the safe harbour under DMCA is lost, intermediaries may still claim immunity and are protected under the CDA.

4.2.2 India

In India, Section 79 limits the defence provided to intermediaries from liability for third party content on their failure "to expeditiously remove or disable access to that material on that resource without vitiating that evidence in any manner."[208] The Rules issued in 2011, state that intermediaries "shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2)."[209] At the time of the enactment of the time period specified under the Rules was deemed too short

---

[206] Subrule (E), Rule 2 Conditions, Section 512 DMCA
See:http://www.copyright.gov/title17/92chap5.html#512

[207] CARDOZO ARTS & ENT. L.J. 'Defining Expeditious, Unchartered territory of the DMCA safe harbour provision-A survey of what we know and do not know about the expeditiousness of service provider responses to takedown notifications', (2008-09); J.D. Candidate 2009, Benjamin N. Cardozo School of Law; honors include Dean Merits Scholar, Public Service Scholar, and Heyman Scholar. B.A. from Yale University (2004)See: http://www.cardozoaelj.com/wp-content/uploads/Journal%20Issues/Volume%2026/Issue%202/Weinstein.pdf

[208] Section 79 3(b) IT (Amendment) Act India "upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

[209] See Sub rule (4) IT Act India Intermediaries Guidelines Rules 2011 *supra note 79*

for assessing and restricting content. Subsequently, the government clarified[210] that 36 hours was the time frame for the acknowledgement of receipt of the notice for taking down content and does not specify the actual time frame for taking down the content.

4.2.3 Canada

In Canada, as the liability of the intermediary is limited to forwarding the notice, Section 41.26 under CMA specifies that the intermediary upon receiving must forward the notice to the alleged infringer identified by the rights holder "as soon as feasible" and "inform the claimant of its forwarding or, if applicable, of the reason why it was not possible to forward it".[211]

4.2.4 United Kingdom

In the UK, under the ECD Regulations 2002 mere conduits are exempted from liability to take action and under Section 18 and Section 19 specifies that hosting and caching intermediaries must act "expeditiously" to seek the safe harbour defense.[212] The directive gives no guidance as to what expeditious means, however, and whether it allows enough time to check the validity of a claim. In the UK Mumsnet case, for example, the defendants settled, apparently because they were unsure whether even removal within 24 hours was expeditious.[213] Further, under UK law the ECD Regulations provide which provide specific immunities for service providers from offences under the Terrorism Act 2006[214], do prescribe that take-down must take place within two days.

The accompanying regulations to the Defamation Act clarify that the intermediary must take action within 48 hours though under certain circumstances this may be extended as decided by the court.[215] The Regulations specify 48 hours for taking action on part of the intermediary including forwarding notice to poster of the statement, acknowledging that complaint has been received to the complainant.[216] The intermediary must also remove the alleged defamatory statement within 48 hours on not being able to contact the original poster or if the poster fails to contest the statement or if the poster agrees to remove the statement.

---

[210] Government of India Ministry of Communications and Information Technology, Department of Electronics & Information Technology, (March 18, 2013) See: http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules_1.pdf

[211] 41.26 (1) (a) *supra note 94*

[212] Section 18 and Section 19 ECD Regulation 2002 UK *supra note 57*

[213] Clarinette, 'The eCommerce Directive: A shield for ISPs…. Or a stick with which they may be beaten?', (February 20, 2013) See: https://clarinettesblog.wordpress.com/2013/02/20/the-ecommerce-directive-a-shield-for-isps-or-a-stick-with-which-they-may-be-beaten/

[214] Terrorism Act 2006 c. 11 UK, see http://www.legislation.gov.uk/ukpga/2006/11

[215] Schedule Defamation Act, Regulation 5 for the Operator of Websites, http://www.legislation.gov.uk/uksi/2013/3028/schedule/made

[216] Section 2 and 3 *Ibid. 183*

In case the poster contests the claims then the intermediary must inform the complainant in writing within 48 hours and in case of repeated infringements must remove content specified in the locations in original notice within 48 hours. The poster of the statement has a limited time frame which cannot exceed the fifth day from the issuing of the notice to respond to the complaint. Under the DEA, knowledge of the infringement through a CIR must be brought forward to the ISP "within the period of 1 month beginning with the day on which the evidence was gathered."[217] Further, sub rule 5 states that, "a notification under subsection (4) must be sent to the subscriber within the period of 1 month beginning with the day on which the provider receives the report."[218]

4.3 Objective/subjective standard

Not all intermediaries may have the sufficient legal competence or even the resources to deliberate on the legality of an expression. When defence from liability is tied to the intermediary taking action upon the alleged content they might end up erring on the side of caution. Even if such intermediary has sufficient legal competence, it has a tendency to prioritise the allocation of its legal resources according to the perceived importance of impugned expressions.[219] Further, if such subjective determination is required to be done in a limited timeframe and in the absence of adequate facts and circumstances, the intermediaries have no choice but to mechanically (without application of mind or proper judgement) comply with the takedown notice.

For an objective standard to be introduced in determining the validity of the claim the takedown or restriction of content should be funneled through and executive or a judicial order. While this may be a time consuming and not the most efficient way due process in restricting content or access to the Internet should ensure that an objective body is evaluating the purported claim.

4.3.1 India and United States of America

Liability frameworks across almost all the regimes being analysed in this study including USA and India require the intermediary to perform a subjective judicial determination in the course of administering a restriction or takedown.

4.3.2 South Korea

Intermediaries may also have obligations as part of the safe harbour conditions or additional liability to screen for obscene material for example as under Art. 22-3, TBA in South Korea. The OSP is under a direct obligation to filter content by virtue of Art 104, Copyright Act. Art

[217] Sub rule 5 of 124A Obligation to notify subscribers of copyright infringement reports *supra note 60*

[218] Sub rule 5 of 124A *Ibid. 185*

[219] Rishabh Dara, *Intermediary Liability in India:Chilling Effects on Free Expression on the Internet 2011*, 29 (Jan. 30, 2015), http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf.

17, Act on the Protection of Children and Juveniles against Sexual Abuse necessitates detection of Child Pornography by the intermediary. No information in violation of Public Official Election Act can be circulated on the Internet. This has been provided under Art 82-4, Public Official Election Act.

In South Korea, an intermediary has the obligation to screen for obscene material under Art. 22-3, Telecommunication Business Act in South Korea. The OSP is under a direct obligation to filter content by virtue of Art 104, Copyright Act. This section was upheld as constitutional in the case of 23-1(A) KCCR 53, 2009 Hun-Ba13, 52, 110 . Art 17, Act on the Protection of Children and Juveniles against Sexual Abuse necessitates detection of Child Pornography by the intermediary. No information in violation of Public Official Election Act can be circulated on the Internet. This has been provided under Art 82-4, Public Official Election Act.

4.3.3 United Kingdom

Under graduated response scheme defined under the DEA in the UK, the power to make provision about injunctions preventing access to locations on the internet is limited to regulations made by the Secretary of State.[220]

4.3.4 Chile

In Chile, no level of proof is required specifically in copyright law; however, reasoned decisions are the general rule for all judicial orders and decisions. In the same fashion as DMCA, there are no obligations to cut off connection, though one of the conditions to seek defence from liability is that the service provider sets general policies for service termination for repeat infringers. There have been no voluntary industry solutions to deal with repeated infringers, nor graduated response schemes.

4.4 Due process

Balanced liability frameworks must provide due process including establishing a prescribed level of proof for takedown and requiring an intermediary to give a reasoned explanation for restricting or taking down content or for cutting off access.

4.4.1 United Kingdom

In UK the amendments to the 2013 Defamation Act raises the threshold for defamation cases by introducing the requirement of 'serious harm'. Section 1 states, "a statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant."[221] Subsection (2) provides that commercial bodies will have to demonstrate actual or likely serious financial loss.[222] Section 2 establishes "defence to an action

[220] Digital Economy Act, S. 17 (2010). *supra note 60*
[221] Section 1(1) Defamation Act UK 2013 *supra note 49*
[222] Section 1(2) *Ibid. 189*

for defamation for the defendant to show that the imputation conveyed by the statement complained of is substantially true."[223]

Defendants may benefit from this defence where it can be shown that the imputation was 'substantially true', following case law which has held that defendants do not have to prove the truth of every individual word.[224] Section 3 further states the proof of "honest opinion" reflecting the current law except the requirement to prove that the statement is an opinion of "public interest".[225] Section 4 introduces a defence for when a statement is a matter of public interest and where the defendant also reasonably believed the publication was in the public interest.[226]

Under the DEA, the copyright owner bears the burden to track and identify infringements. The ISP has to follow a strict procedure upon receiving notice of an infringement, including the information that must be be included in the CIR that the rights holder sends out to the intermediary.[227] Provisions specifying the content of a legitimate notice also state that the copyright owner must specify "information about subscriber appeals and the grounds on which they may be made".[228] The intermediary identifies the user, upon receiving the location of the alleged unlawful activity and forwards complaint to the user.

The CIR serves as a notification of infringement on part of the rights holder and under the initial obligations suffices as the proof needed for the intermediary to send forth the letter of warning.[229] Denial of access to internet, may only be authorized, once the minimum threshold of CIRs have been filed and other factors have been fulfilled.[230] The ECD Regulations do not specify a prescribed level of proof nor does it require a reasoned decision to be given to the user by the intermediary.

4.4.2 India

In India there is no prescribed level of proof, nor is the intermediary required to give a reasoned decision for taking down or restricting content. The Indian regime does prescribe a mandatory content policy which contains an exhaustive list of types of expressions which are not permissible.[231] However, it should be noted that even though terms like 'objectionable', 'hateful' and 'disparaging' are stated as not permitted these have not been defined anywhere in

[223] Section 2 Truth Defamation Act 2013 *supra note 49*
[224] Nick Mathys and Oliver Neil, Defamation Act 2013 comes into effect (Jan. 7, 2014) http://www.lexology.com/library/detail.aspx?g=cc6db7c1-8ed8-484a-ad2d-505a450fdb3.
[225] Section 3 'Honest Opinion' Defamation Act 2013 UK *supra note 49*
[226] Section 4 'Publication on matter of public interest' Defamation Act 2013 UK *supra note 49*
[227] See 124 A, Digital Economy Act, (2010). *supra note 60*
[228] 124 A 6 (e) Digital Economy Act, (2010). *supra note 60*
[229] Ibid 196
[230] Section 17(3)Power to make provision about injunctions preventing access to locations on the internet Digital Economy Act, (2010). *supra note 60*
[231] Rule 3(2) Intermediary Guidelines 2011 supra note 79

the Rules. This content criteria constitutes as a criteria for takedown and functionally serves as a threshold of proof. The Indian legislation is the only legislation to require a mandatory content policy as part of the intermediary's due diligence requirements to seek the defence of safe harbour. Further, the Indian regime allows for service providers to create provisions that may restrict or cut off access to the Internet under their policy.

4.4.3 Canada

In Canada the CMA also does not specify a prescribed level of proof for ISSP to forward notice of infringement and as long as the intermediary has received a notice of the infringement from the rights holder and they forward it to the alleged infringer they may claim defence. As the liability of the intermediary is limited to passing the notice to the alleged infringer

4.4.4 United States of America

In the USA the DMCA requires only the identification of copyrighted work by the rights holder to be sufficient as the proof of an infringement and the intermediary has obligations are linked to taking action upon receiving the notice. There is no requirement to give a reasoned decision on part of the intermediary under the DMCA and there are no obligations on the service provider to cut off connection, though section (i) could be potentially be interpreted as a graduated response scheme. The section states that since it states that one of the conditions to seek defence from liability is the service provider provides for termination under appropriate circumstances or for repeat infringers. This has so far, been interpreted by the courts and has led to development of voluntary industry solutions to deal with repeated infringers.[232]

4.4.5 South Korea

The prescribed level of proof for take down in South Korea is similar to as provided in the US; it requires identification of the copyrighted work. Under the Public Official Election Act any information in violation of Public Official Election Act on the Internet requires it to be taken down. The Service Provider needs to give a reason for take down of information such as obscenity for taking down Child Pornography. However, under the ICNA(Information and Communication Network Act) requires that an intermediary immediately take down content upon receiving a complaint without looking into whether the information is actually right infringing or not. This sometimes leads to deletion of lawful content as well. Due Process can also lead to termination of user account under Art 8, KCCA.

[232] Masnick Mike, Music Publishers, With Help From Rightscorp, Test Legal Theory That DMCA Requires Kicking Repeat Infringers Off The Internet, Tech Dirt (December 1st, 2014) See: https://www.techdirt.com/articles/20141128/05045629270/music-publishers-with-help-rightscorp-test-legal-theory-that-dmca-requires-kicking-repeat-infringers-off-internet.shtml

4.4.6 Chile

In Chile, any person authorised on behalf of the rights holder can bring forward a claim. The intermediary has to either block or remove the content expeditiously if it is infringing copyright or related in any manner, as mandated through a court order. This involves ascertaining the prescribed level of proof which is: Identification of infringed rights, rights holder, form of infringement, infringing material and location. The intermediary is not required to give a reasoned explanation for taking down any content in Chile.

4.5 Procedural safeguards

No matter what the procedure for restricting content, it should follow certain procedural safeguards such as prescribing a government registered agent for handling notices, informing users if their content has been taken down. Further a balanced regime must always and following the rules of natural justice by providing the third party content creator should be given the right to be heard. Also if content has been taken down then there should be mechanism in place to put back content including appeal to a higher authority and users should be informed of the time delay before the content may be restored.

4.5.1 United Kingdom, India, Canada and United States of America

Apart from the framework set forth under the ECD, which does not provide for the signature of the claimant being a mandatory part of the notice all other regimes under the study, do specify the claimant's signature as proof. Only the Indian regime and the US regime create provisions for the appointment of a designated officer to administer takedowns.[233] While under the DMCA the officer must be registered with the government, there is no such requirement under the Indian legislation.

4.5.2 India

The Indian regime and the ECD Regulations do not specify that the third party content creator or user must be informed of the takedown however, several other legislations do specify this. The Copyright Act specifies that in case the copyright owner complaining of infringement fails to produce orders from the court in the infringement suit, the content may be put back by the intermediary within 21 days. However, the user is not informed of the takedown unless he wants to access the allegedly infringed content.

4.5.3 United States of America

The DMCA does specify that after the content has been taken down the user needs to be informed. DMCA also provides for a mechanism for putting back content that was wrongfully taken down within a period of 10 to 15 days.

[233] IT Act Intermediary Rules 2011, *supra note 79* and Section 512 DMCA *supra note 23*

4.5.4 United Kingdom

Under the graduated response scheme of the DEA, the subscriber who has been alleged of an infringement is provided all relevant details pertaining to the alleged infringement including the evidence gathered and relevant legal advice.[234] There is no mechanism to put back content under the DEA.

4.5.5 Canada

In Canada, under the CMA if the service provider does not forward the notice they have to notify the complainant as to why the notice was not forwarded.[235] In UK the Defamation Act the consent of the user is taken before taking down content or as per court order.[236] Under the DEA, the user informed of notice, and is given all relevant details, such as details of alleged infringement, evidence gathered, relevant legal advice for current and future situations and the legislation also provides a mechanism for grounds of appeal, etc.[237] Further, as per Section 3, the "obligations code" must have a due process for grounds of appeal as per section 13.[238]

The DEA provides the notification from the ISP must inform the subscriber that the account appears to have been used to infringe copyright, give the name of the copyright owner who has provided the report, provide evidence of the apparent infringement, direct the consumer towards legal sources of content, include information about subscriber appeals and the grounds on which they may be made, and provide other information.[239]

It also requires ISPs to make available advice on protecting internet access services from unauthorised use, taking into account that different protection will be suitable for different subscribers such as, for example, domestic subscribers, libraries, and small and medium business. The code may require the notification to include other material as well, such as a statement that information about the apparent infringement may be kept and disclosed to the copyright owner in certain circumstances. Further apparent infringements using the subscriber's account may result in additional notifications.[240] All regimes are limited in their transparency standards, with no specific provisions mandating the intermediaries to disclose the takedowns. The Canadian regime mandates storing of identification details upto 6 months to a year after notification.[241]

---

[234] DEA 124A (4) "An internet service provider who receives a copyright infringement report must notify the subscriber of the report if the initial obligations code requires the provider to do so."

[235] Copyright Modernization Act, *supra note 94*

[236] Defamation Act 2013, *supra note 49*

[237] Digital Economy Act 2010, *supra note 60*

[238] Section 3, Digital Economy Act 2010, *supra note 60*

[239] Digital Economy Act 2010, *supra note 60*

[240] Digital Economy Act 2010, *supra note 60*

[241] Sections 41.25-41.27, Copyright Modernization Act, *supra note 94*

4.5.6 South Korea

In South Korea, the Korea Communication Standards Commission (KCSC) is responsible for handling the notices. The user is supposed to be informed under Art 103 of the Copyright Act and Art 21 of KCCA. Appeal can be made to a higher authority against the takedown under Art 103-3, Copyright Act i.e.from the OSP to the Minister of Sports, Culture and Tourism. IA similar redressal mechanism is also provided for under Art 82-4, Public Official Election Act (Only for election campaign) and Art 21, KCCA.

4.5.7 Chile

A third party is not explicitly afforded an opportunity to be heard by the intermediary before a court requires removal or blocking, though it is not strictly forbidden. A counter notice can be filed and appeal can be made to the higher authority. Limitation of liability is established for removal after judicial notice. Such a rule is not present regarding mere conduits; however, courts may still order blocking (Art. 85 R) to those intermediaries.

4.6 Data retention and data disclosure requirements

Depending on the type of regime, there may be different communication or disclosure obligations that are placed on intermediaries. Some distinctions are important to bear when considering communication, disclosure and monitoring obligations of the intermediary.[242]

Monitoring obligations conditional to which a defense of immunity may be claimed on part of the intermediary, may lead to removal or restriction of illicit content without a request and there may be certain communication obligations placed on the intermediary in relation to these monitoring related restrictions, though this may not always be the case. Further disclosure obligations may be placed on the intermediary by the government or through an agency or through court sanctioned private party requests.[243]

Communication and disclosure obligations are also closely linked to data retention obligations, though retention mandates are not always linked to communication obligations. Further, there may be other parallel legislation that set out communication and disclosure obligations across a broad range of areas such as telecommunication law, intellectual property and codes of criminal procedures among others. There may also be separate provisions within the same regime related to data protection as is the case in EU.[244] Any balanced liability framework must distinguish between these overlaps and set clear requirements for the intermediary in relation to each type of obligation.

---

[242] Study on the liability of intermediaries, *supra note 123*

[243] *Ibid.*

[244] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 - 0050 See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

The study on the liability of the intermediaries across EU distinguishes on the basis of four kinds of communication related obligations,

- Obligations to actively inform public authorities
- Obligations to provide information at request of public authorities
- Obligations to provide assistance for interception by public authorities
- Claims for disclosure of information brought by private right holders

4.6.1 India

In India under the NTD regime established under the IT Act and Rules, and the Copyright Act 1957 and the Copyright Amendment Act of 2012, there are no specific provisions for logging of users' identification details or details of information accessed by the user. The intermediary must retain records related to information that was taken down up to 90 days.[245] However, the regime does place disclosure obligations on the intermediary under provision (7) of the Rules that specify, "When required by lawful order, the intermediary shall provide information or any such assistance to government agencies who are lawfully authorised for investigative, protective, cyber security activity."

Further, the provision goes on to state that the "information or any such assistance" shall be provided for the "purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force..".[246] The law also specifies that any request for such information or assistance is pursuant to a written request that clearly states the purpose why this information or assistance is required.[247] However, it does not provide limitations on intermediaries for the storing, sharing or using the information gathered, nor are any specific data retention provisions included.

4.6.2 United States of America

In the USA, the DMCA does not lay out a specific provision for logging of users' identification details or the logging of information accessed by the user. However, under section (h) provides for copyright owner or person authorised to act on their behalf to seek identity of alleged infringer from the ISP with a subpoena issued from the court.[248] The provision states that following the subpoena, an ISP must disclose "sufficient information" for the copyright owner or agent authorised on their behalf to be able to "identify the alleged

[245] Sub rule 4 Intermediaries guidelines (2011) India *supra note 78*
[246] Sub rule 7 I*bid.*
[247] Proviso to Section 52(1)(c), The Copyright Act, 1957
[248] (h) Subpoena to Identify Infringer, § 512 DMCA *supra note 23*

infringer of the material described in the notification to the extent such information is available to the service provider." The ISP must provide the information sought under the subpoena regardless if they acknowledged the notification of the alleged infringement. The regime in US does not lay out any specific provisions for intermediaries to share information related to cyber security incidents or other identified illegal activities.

4.6.3 United Kingdom

In EU, the ECD 2000 under Article 15 'Prohibition of a general monitoring obligation' states:"Member State shall not impose a monitoring obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."[249] Further, under sub rule (2) of Article 15, member states may establish obligations for ISSPs to inform public authorities of alleged illegal activities undertaken or upon information provided by recipients of their service or to communicate to competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.[250]

In the UK the Regulation does not incorporate this sub rule, there are general rules regarding request for information. The UK imposes in specific cases obligations to report communication details to the authorities, e.g. in compliance with a warrant issued under Section 5(1)(a) of the Regulation of Investigatory Powers Act 2000[251] to secure the interception of a communication in the course of its transmission by means of a telecommunication system. Further private Norwich Pharmacal-type actions, directed against access providers, platform operators, and search engines dealing with disclosure of names and addresses of recipients of services allegedly involved in unlawful behaviour have been brought against intermediaries in several cases in UK and Ireland. Under this rule, a third party that is not involved in litigation though has information relating to unlawful content, a court could compel the third party to assist the claimant or suffering party by disclosing information in their possession that is related to unlawful behaviour. Third party may claim reasonable costs of producing the information if a court order is made. However, it should be noted that under Irish data privacy laws intermediaries may share user information only following a court order.

In 2005 in *EMI v Eircom*[252] a Norwich Pharmacal-type action was brought by record companies in order to compel ISPs to identify users accused of file-sharing. The courts upheld

[249] *ECD 2000 Supra note no. 22*

[250] *Ibid. 202*

[251] Regulation of Investigatory Powers Act 2000 c.23 See: http://www.legislation.gov.uk/ukpga/2000/23/section/5

[252] EMI Records (Ireland) Ltd -v- Eircom Ltd [2005] IEHC 233

that ISPs acted within the law by not volunteering this information because "they owe duties of confidentiality to their subscriber." Further the court clarified that, "whilst the court has jurisdiction to make the orders sought it is a jurisdiction which falls to be exercised sparingly. It involves the court in balancing the rights of the Plaintiffs with the obligations of the Defendants towards their subscribers and the rights of those subscribers. These obligations are obligations of confidentiality or privacy. These duties of confidentiality owed by the Defendants to their subscribers and the subscribers entitlements may arise under statute, by contract or at common law."

In 2014, in *Hegglin v. Person Unknown & Google Inc.*,[253] English High Court allowed the service of papers on Google Inc. in California, outside the English jurisdiction, based on the claimants appeal that their data protection and privacy rights had been infringed on by the search engine. The court granted a Norwich order against Google Inc. so that the claimant could identify the unknown persons that were alleged to have posted defamatory statements against the claimant.

The disclosure mandates for intermediaries in relation to Defamation in the UK, is far from being settled. The 2013 Defamation Act, introduces under Section 10, a further defence for intermediaries who are not the author, editor or publisher of the alleged unlawful statement. The Section states that the court "does not have jurisdiction to hear and determine an action for defamation brought against a person who was not the author, editor or publisher of the statement complained of unless the court is satisfied that it is not reasonably practicable for an action to be brought against the author, editor or publisher".[254] However, it is unclear from the provision when and how is "not reasonably practicable' to be proved or interpreted. It also does not clarify to what extent does the claimant need to go before the intermediary becomes liable and how this will apply to Norwich Pharmacal orders.

Under the DEA, Section 124A sub rule 3 sets out content of the notifications required by qualifying ISPs which receive CIRs, including to identify the subscriber to which the CIR relates and send notifications as required by the Code, unless the CIR is out of date or it is not possible to do. The initial obligation codes under the DEA also place an obligation on the ISP to send notification that must include information on steps the subscriber may take to protect themselves from unauthorised use of their data by the ISP.[255] Further, in general or particular cases notifications may also include:

a) a statement that information about the apparent infringement may be kept by the internet service provider;

[253] Hegglin v. Person Unknown & Google Inc. [2014] EWHC 2808 (QB)

[254] Defamation Act 2013, *supra note 49*

[255] Digital Economy Act 2010, *supra note 60*

b) a statement that the copyright owner may require the provider to disclose which copyright infringement reports made by the owner to the provider relate to the subscriber;

c) a statement that, following such a disclosure, the copyright owner may apply to a court to learn the subscriber's identity and may bring proceedings against the subscriber for copyright infringement; and

d) where the requirement for the provider to send the notification arises partly because of a report that has already been the subject of a notification under subsection (4), a statement that the number of copyright infringement reports relating to the subscriber may be taken into account for the purposes of any technical measures.

Also Part 4 of the Code places obligation to provide infringement lists if requested by the copyright owner or set out as part of the initial obligations . This would require a qualifying ISP to establish procedures for the accurate identification of subscribers from IP addresses specified in CIRs. The provisions specify that the infringement list should set out in relation to each relevant subscriber, which of the copyright infringement reports made by the owner to the provider relate to the subscriber, but does not enable any subscriber to be identified. However, consultations with stakeholders regarding the implementation of these data retention and disclosure provisions have raised several practical issues around costs, invalid CIRs and when subscribers have left the ISPs service.

4.6.4 Canada

The regime in Canada mandates the retention of records that "will allow the identity of the person to whom the electronic location belongs to be determined..".[256] Further, from the day that the intermediary receives notice of the claimed infringement they must retain records for six months. This retention period may be extended upto a year if the claimant commences proceedings relating to the claimed infringement and so notifies the person before the end of those six months. Since 2000 courts have interpreted, defined and clarified disclosure requirements for ISPs in relation to a broad variety of issues

In 2000 *Irwin Toy v Doe*,[257] the Ontario Rules of Civil Procedure were successfully were applied to obtain a disclosure order. The plaintiff traced defamatory emails sent to employees to particular IP addresses belonging to ISP company iPrimus that was required to reveal the owners of the IP addresses in question. Further the court noted that ISPs do not have an obligation to disclose user information without a court order. In 2004, in *BMG Canada v John Doe*[258] the Federal Court of Canada heard an appeal from the representatives of the recording

[256] Section 41.25 (1)(b) of the Copyright Modernization Act, *supra* note 94

[257] Irwin Toy Ltd v Quebec (AG), [1989] 1 S.C.R. 927

[258] BMG Canada Inc. v John Doe, 2004 FC 488

industry seeking various ISPs to disclose subscriber information of users using P2P networks to share and download copyrighted music files. The court denied the appeal determining that any order for disclosure of subscriber information must balance subscribers privacy rights and that the copyright owner must show a bona fide claim, and held that in this case the privacy concerns outweighed the disclosure.

The next important clarification of disclosure standards of intermediaries came in 2009, when the Ontario Superior Court granted a Norwich Pharmacal order against ISPs to disclose subscriber information so that defamation charges could be taken forward. The court in granting a Norwich order considered, if there was enough evidence to raise a bona fide claim, whether the third party that information being sought from is involved in the acts complained of, if third party is the only practical source of information available, whether third party can be indemnified of costs that may incurred in the disclosure of information and whether it is the interest of justice to favour obtaining the disclosure. [259] (para 13)

Further in 2010, the Ontario Superior Court in *Warman v Fournier*[260] ruled that disclosure of users' identities should not be automatic. The ruling considered an established prima facie case against the unknown wrongdoers, complainant's acting in good faith and, whether they have taken reasonable steps to identify the unknown party, and whether the public interests favouring disclosure outweigh the legitimate interest of freedom of expression and right to privacy (para 34). Further it added another factor for consideration for requirement of disclosure that is whether the unknown users could have a reasonable expectation of anonymity given the context.

Most recently, in *Voltage Pictures v Does*[261] in 2014, the Federal Court of Canada granted disclosure order to claimant seeking 2000 users from an ISP. The Court ruling was based on the claimant showing that the bona fides claim and privacy rights of the users did not outweigh the interests of the copyright holders. The court however, outlined several safeguards against possible invasions of privacy including though not restricted to users' information not being made available for public use, or for any other use and claimant had to bear the ISPs legal expenses and courts would review any demand letters being sent forth from claimant's to users.

4.6.5 South Korea

In South Korea, the Korea Communication Commission can order to restrict, limit or suspend any illegal information which has the potential of aiming or abetting any crime. Under Art 21, KCCA the KCC can deliberate on such matters and issue correction requests as well. However, no retention mandates exist as part of the intermediaries' obligations.

---

[259] York University v Bell Canada Enterprises, 2009 99 OR (3d) 695 (ONSC)

[260] Warman v Fournier et al, 2010 ONSC 2126 (Div Ct)

[261] Voltage Pictures v Does, 2014 FC 161 See: https://cippic.ca/uploads/Voltage_v._Does-2014FC161.pdf

4.6.6 Chile

In Chile, the law provides for the copyright owner, or person authorised to act on their behalf, to seek the identity of alleged infringer from the ISP with a subpoena issued from the court. The ISP must disclose information "that allows to identify the alleged infringer by the service provider". It does not specify to whom such information must be delivered, or for what purpose.

None of the regimes have established cooperation obligations for intermediaries to provide assistance for interception by the government or its agents.