LAURA C. RODRIGUEZ RENGIFO

INTERNET INTERMEDIARIES LIABILITY:
Participative Networking Platforms and Harmful Content

LLM RESEARCH PAPER

LAWS 530: FREEDOM OF EXPRESSION AND CENSORSHIP

FACULTY OF LAW

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

2016

Contents (References - table of contents)

Abstract

This paper proposes a new conceptual approach to the issue of Internet Service Intermediaries' (ISIs) liability by classifying these agents into Authority Gatekeepers and Micro-Gatekeepers. This classification aims to give a better understanding of ISIs role on the new online chain of communication and their responsibility for harmful content created by third parties. This paper analyses from a critical perspective how legal sources have addressed the liability of one type of ISIs, Platform Networked Providers (PNP) such as Facebook, for harmful digital communications and proposes a new way to deal with this problem in order to balance Freedom of Expression and effectively deterring harmful speech.

Word length

7512 words.

Subjects and Topics

Internet Intermediaries Liability
Participative Networked Platforms
Gatekeepers and democratization of the speech
Safe harbour .
Harmful Digital Communication Act 2015
Facebook Host
E-commerce Directive 2000.

I Introduction

Over the last number of years there has been a critical shift in the way information is communicated to (and between) individuals.[1] Before the Internet was easily accessed, content and speech was moderated by the traditional "gatekeepers", a centralized collection that had the ability to moderate content and decide what shall be published and what should not, for instance; publishers, broadcasters, newspapers, among others. The internet and its agents have been replacing these centralized gatekeepers conceptually changing the communication chain.

The new decentralization and democratization of speech facilitated by the Internet, is achieved by allowing individuals not only to be creators of the information but to be gatekeepers as well. A new chain of online communication is composed by the author. The infrastructure provider (Authority Gatekeepers), the platform (Authority gatekeepers), small intermediary (Micro-Gatekeepers e.g. Facebook Page Administrator) and finally the receptor who can be a creator of speech as well. This paradigm is feasible in part due to the functionalities of Participative Networked Platform (e.g. Facebook).This paper deals only with Participative Network Platform that host user-generated content online.

Although this paradigm is fructiferous for democracy because it allows a high participation of individuals in political and social speech[2], in jurisdictions around the world (including New Zealand), there is a growing concern about harm in Cyberspace. Legal threats online is a wide-ranging topic, elongating into different areas of law, from defamation to copyright infringement[3]. One of the hardest challenges for legal sources when addressing these issues is to detect who was liable for the harmful content.

The root of these issues is the incapability of law to outpace the technology innovations. In other words, legal sources have failed to translate the reality behind technology into legal

[1] See Jürgen Habermas "Political Communication in media society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research" (2006) 16 CT 411 at 423.

[2] See also Emily Laidlaw "Internet Gatekeepers, Human Rights and Corporate Social Responsibilities" (Doctor of Philosophy thesis, London School of Economics and Political Science, 2012) at 25. Retrievable from <http://etheses.lse.ac.uk/317/>

[3] Law Commission *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (NZLC SP23534, 2012) at 1.

grounds in order to know who is responsible for harmful content. This paper will addresses exclusively harmful contend uploaded by third parties.

In an attempt to catch up with technology, jurisdictions have enacted "digital bills" to address specifically issues on the Internet such as harmful content. For instance, In New Zealand, the Harmful Digital Communications Act 2015, has been enacted to deter online content that can lead to cyber bullying, defamation, hateful speech and blasphemy among others. But, how effective is this legislation depends on how accurate to technology dynamics it is. As stated above and to illustrate, in terms of liability a Facebook page hosts is not the same as Facebook the platform. Despite how much impact this differentiation may have, it has not been taken into account by law makers or case law in New Zealand.

This paper proposes a new way to understand the role of every agent in the chain of communication by applying the sociological theory of the "Network Gatekeeping" proposed by Barzilai-Nahon[4]. This theory proposed that ISIs are classified in Authority Gatekeepers and Micro-Gatekeepers[5]. Although it is a novel way to analyse the participation of agents over the Internet it leads to a better and more accurate understanding of liability for harmful content uploaded by third parties.

This paper is delivered in four main sections: The first section explores the concept of Internet Services Intermediaries (ISI) and their role as gatekeepers of information from a sociological point of view. The second section is a comparative study between Europe and New Zealand regarding the liability model for ISIs. This section comprehends an analysis of the legislation and case law. This paper concludes that in order to design an effective framework, law makers should take into account the conceptual differences between ISIs.

A Scope of this Paper.

Due to the multiple classification of ISIs, this paper focuses on Participative Networked platforms explained below. Additionally limits its scope to harmful content uploaded by third parties. It leaves aside for a posterior debate other concerns such as copyrights infringement, privacy breaches and other law proscriptions.

---

[4] See Karine Barzilai-Nahon "Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control" (2008) 59 JAmSocInfSci 1493.

[5] Laidlaw, above n 2, at 59.

II Internet Services Intermediaries as Gatekeepers of the Information Flow.

This section explores from a sociological perspective how ISIs have changed the chain of communication and why these changes are important when studying liability for harmful communication. First it explores, the concept of gatekeepers before the internet, the role of ISIs as Gatekeepers, specifically Participative Networked Platforms and third the implications in the analysis of liability.

A Gatekeepers in an Online World : Basic Concepts

Gatekeepers of information and their role in democracies is an obligatory theme of study when referring to both, the right of Freedom of Expression and ISIs' Liability. This is because, they exercise censorship to a certain degree on individuals' speech. First of all, at a general level gatekeepers are entities that exercise information control by, "selecting which information to publish, or channelling information through a channel, or deleting information by removing it, or shaping information into a particular form"[6]. The traditional concept of gatekeepers was studied by literature of Information Science before the penetration of the Internet into the average household. Management, Sociology and Communication discussed how some agents can decided what information shall or not reach certain audiences[7]. For instance, from the communication research perspective, "gatekeepers" were agents who control what information was distributed such as stores, publishing houses, censors, newspaper editors, financial brokers, even national governments[8].

Traditional Gatekeepers have been gradually replaced by new actors online, the so called ISIs. ISIs in the most generic way are those entities providing services that enable individuals to receive or impart information on the Internet[9]. These new Gatekeepers have changed profoundly the chain of communication, but these changes are explored below.

---

[6] "In sociology literature gatekeepers this are those who guard and preserve a community's information": Barzilai-Nahon, above n 4, at 1493.

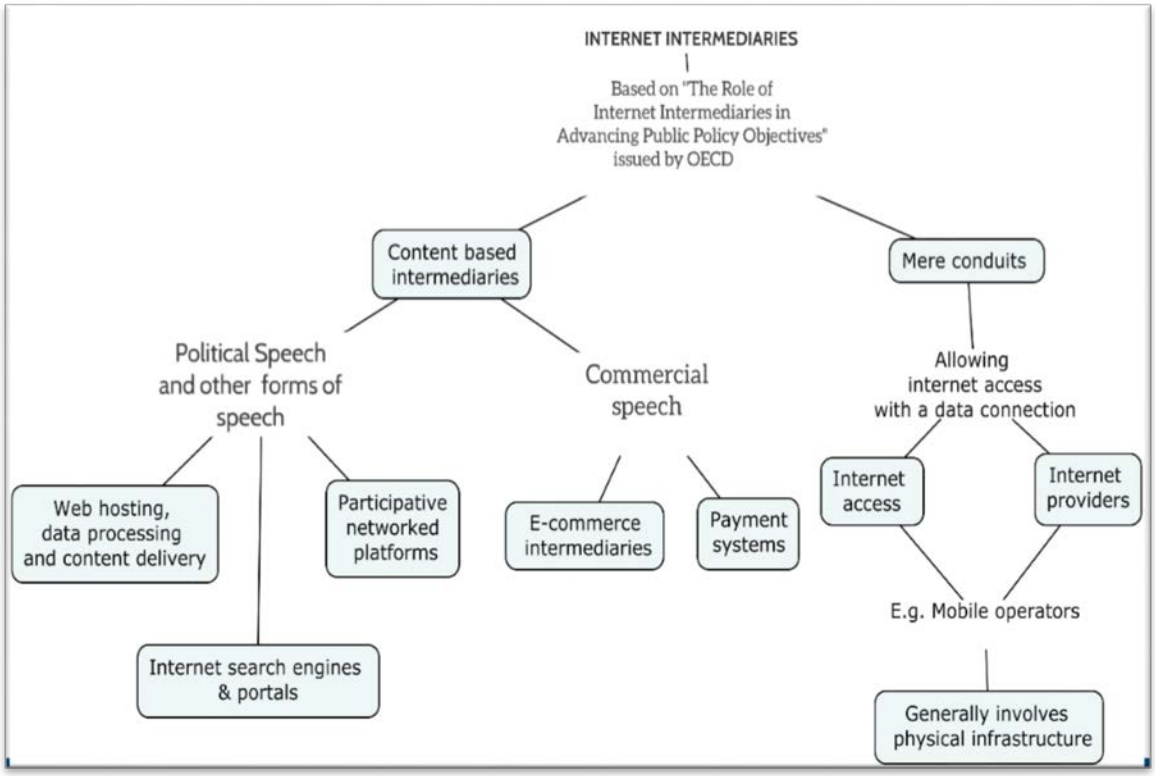
[7] At 1494

[8] *See*, John Perry Barlow "A Declaration of the Independence of Cyberspace" (8 February 1996) Electronic Frontier Foundation <https://projects.eff.org/~barlow/Declaration-Final.html>

[9] Nicolo Zingales "The Brazilian approach to internet intermediary liability: blueprint for a global regime? Internet Policy Review" (2015). 4 IPR 1 at 2 < http://policyreview.info/articles/analysis/brazilian-approach-internet-intermediary-liability-blueprint-global-regime>.

According to the OECD, ISIs role is to "provide the Internet's basic infrastructure and platforms by enabling communications and transactions between third parties as well as applications and services"[10]. Additionally, they "give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties"[11]. There are two main categories of ISIs[12]. 1. Dumb pipes: These are "meant to signify Internet access providers, which provide subscribers with a data connection allowing access to the Internet through physical transport infrastructure"[13] (e.g. Vodafone). This are classified as "mere conduits" or dumb pipes because they just provide the infrastructure. The second is the "content based intermediaries" "whose business model depends on the publication of "quality" content" [14] (e.g. Facebook and Yahoo). This ISIS are categorized in the next diagram according to their technology architecture[15].

Diagram 1. Classification of ISIs according to their technology features.



[10] OECD "Economic and Social Role of Internet Intermediaries" (April 2010), available at <http://www.oecd.org/officialdocuments> At 9.

[11] At 9.

[12] Zingales, above n 9, at 3.

[13] OECD, above n 10, at 11.

[14] Zingales, above n 9, at 3.

[15] This classification is a mixture based on the OECD model. At [9-14].

This paper focuses only on Participative networked Platforms which can be seen in the Diagram 1 as part of the category "Content Based Intermediaries". The OECD established the concept of Participative Networked platforms as:

> Services based on new technologies such as the web, instant messaging, or mobile technologies that enable users to contribute to developing, rating, collaborating and distributing Internet content and developing and customising Internet applications, or to conduct social networking. This category is intended to include social networking sites, video content sites, online gaming websites and virtual worlds[16].

The OECD breaks down the list of ISIs into categories according to their functionality. Among the listed are Facebook and Twitter which have a large user base.

Diagram 2: Classification of Participative Networked Platforms

Type of Platform	Examples
Blogs	Blogs such as BoingBoing, Engadget, Ohmy News; Blogs on sites such as LiveJournal; Windows Live Spaces; Cyworld; Skyrock
Wikis and other text-based collaboration formats	Wikipedia, Wiktionary; Sites providing wikis such as PBWiki, Google Docs
Instant messaging	Skype, Trillian, Windows Live Messenger
Mobile	Mobile versions of social networking sites and applications such as Facebook
Sites allowing feedback on written works	FanFiction.Net, SocialText, Amazon
Group-based aggregation	Sites where users contribute links and rate them such as Digg, reddit Sites where users post tagged bookmarks such as del.icio.us
Photosharing sites	Kodak Gallery, Flickr
Podcasting	iTunes, FeedBurner (Google), WinAmp, @Podder
Social network sites	MySpace, Mixi, Facebook, Twitter, Bebo, Orkut, Cyworld, Imeem, ASmallWorld
Virtual worlds[23]	Second Life, Active Worlds, Entropia Universe, Dotsoul Cyberpark
Online computer games	World of Warcraft, Tomb Raider, Lineage Ultima Online, Sims Online, Club Pogo[24]
Video content or filesharing sites	YouTube, DailyMotion, GyaO, Crackle

Source: Building on OECD, *Information Technology Outlook 2008, Chapter 5 - Digital Content and Convergence in Transition.*

1 ISIs and their impact in the chain of communication: a Democracy matter.

Before narrowing this study to Participative Networked Platforms, it is necessary establish a few points. First of all, "content based" ISIs (including Participative networked Platforms) have disrupted the traditional chain of communication and therefore have impacted profoundly the right of Freedom of expression and the democracy paradigm itself. The transformations relevant for this study are three:

[16] OECD, Above n 10, at 14.

(a) Democratization of the Speech:

Balkin established that "a democratic culture is a culture in which individuals have a fair opportunity to participate in the forms of meaning making that constitute them as individuals"[17]. Therefore the more access to participation channel individuals have, the more democratization of speech there is in a society. The Internet then, opened spaces to creators of the speech to reach larger audiences, and for audiences to become in authors of information as well (See Diagram 4). The democratization of the chain of communication occurs when there is a common and open protocol used to facilitate direct communication between all users or "ends" connected[18]. For example, the opportunity that Internet users have to create blogs to upload information, or Facebook pages to group individuals with the same interest. At the same time, new interactive forums give the possibility to audiences to participate and reply to the original message.

(b) Decentralization: More Gatekeepers than before,

The centralized model refers to traditional media intermediaries (e.g. Newspaper or Television Channel), who were in a position to highlight preferred content and suppress or ignore unpopular points of view[19]. In contrast with these traditional communication models (see Diagram 3) which has a few noticeable gatekeepers, "Internet communication was based on a peer model"[20]. The power of censorship of the speech is no longer held by a few but a large number of internet agents. "Between every user of the internet and the content being accessed are numerous actors involved in the process of bringing to the user the desired content"[21] (see Diagram 4). "[E]ach of these actors through which a user can access content on the internet is an intermediary"[22] thus a gatekeeper. For instance, the creator of the blog, the author of the Yahoo forum or the Facebook page host. These actors are not anymore large media companies, they are individuals who are internet users at the same time.

---

[17] Jack Balkin "Digital speech and democratic culture: A theory of freedom of expression for the information society" (2004) 79 NYULRev 1 at 3.

[18] Oren Bracha and Frank A Pasquale "Federal search commission? Access, fairness and accountability in the law of search." (2008) 93 CornellLRev 1149 at 1156

[19] At 1156.

[20] At 1157.

[21] Bailey Rishab "Censoring the Internet: The New Intermediary Guidelines"(2012) February EconPolitWkly 1 at 1.

[22] At 1.

(c) More Gatekeepers more information control.

"An intermediary can theoretically exercise control over the flow of content, possibly making it more efficient for them to deal with instances of offending material"[23] . ISIs, as gatekeepers, are often seen as the agent who control the online content. "This is because they are in a position to eliminate access to objectionable material and, quite often, to identify wrongdoers"[24]. To summarise, the next two diagrams depict how the traditional and new chain of communication are structured taking into account all the three characteristics:

Diagram 3: Traditional Chain of Communication:

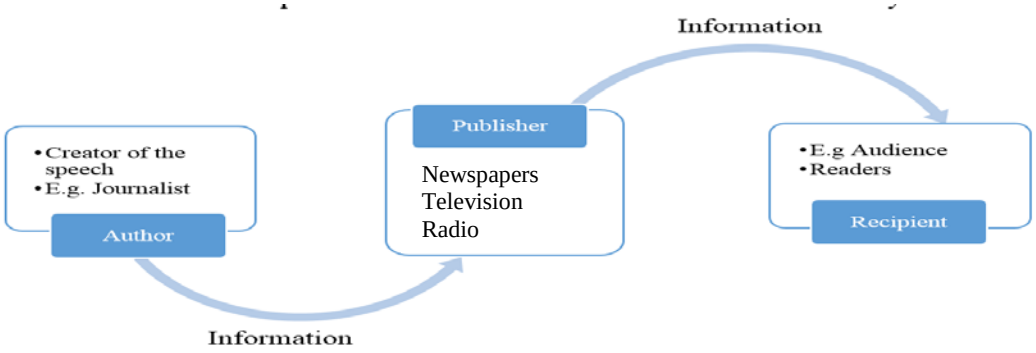
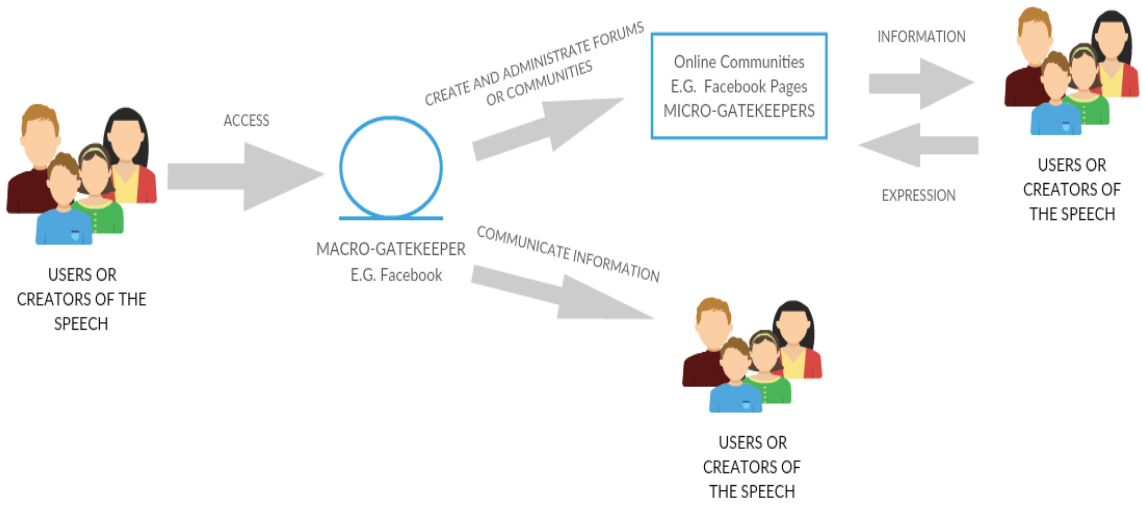


Diagram 4: Online Communication of the Speech:



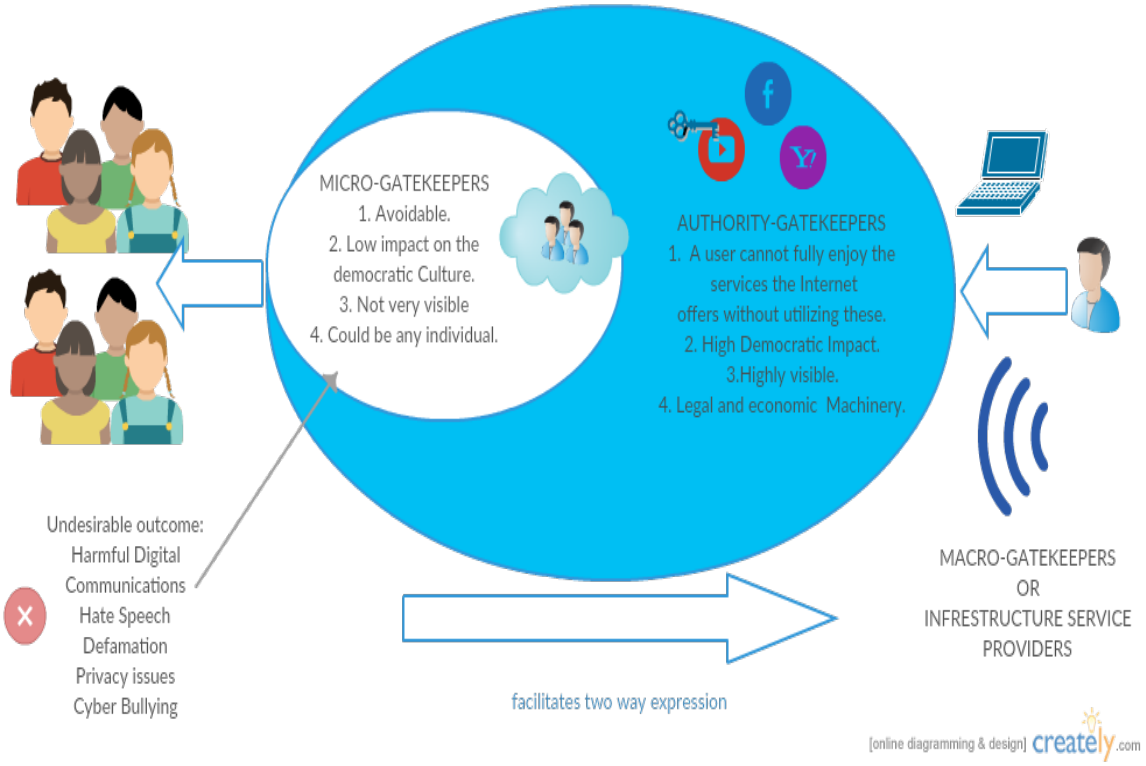
[23] At 1.

[24] Etienne Montero and Quentin Van Enis "Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle?" (2011) 27 CLSRev 21 at 21.

B Layers of Gatekeeping: From Macro, micro-gatekeeper and Authority-gatekeeper.

Another taxonomy of ISIs is explained by Emily Laidlaw who took the theory of gatekeepers proposed by Barzilai-Nahon to differentiate ISIs. "Laidlaw suggests that the human rights obligations of Internet intermediaries should increase according to the extent that their activities facilitate or impact democratic culture"[25]. This categorization seems to be adopted by the European Commission who quoted Laidlaw: "A distinction is made between Micro-Gatekeepers (certain content moderators), authority gatekeepers (Facebook, Wikipedia, portals), and Authority Gatekeepers (Internet Service Providers)".[26] As stated above, Authority Gatekeepers are out of the scope of this research. The focus then is Micro-Gatekeepers and Authority gatekeepers. The next diagram is an illustration of the new chain of communication based on the Laidlaw classification.

Diagram 5: Authority gatekeepers and Micro-Gatekeepers



[25] European Commission *Report on factors which enable or hinder the protection of human rights* at 50 (2014) retrievable from < http://www.fp7-frame.eu/wp-content/materiale/reports/03-Deliverable-2.1.pdf>

[26] Laidlaw, above n 2, at 59. Cited by European Commission, above n 25, at 154.

This classification is just illustrative, and this paper is of the opinion that more sociological research is required to establish categories of ISIs, additionally, it is difficult to strictly categorize agents in a dynamic environment as The Internet is. As Bracha Commented "the technological structure of the Internet is not static. Technology is a plastic medium, open to a broad range of reshaping, entailing various patterns and degrees of control."[27] Therefore, there are agents that initiate their online life as Micro-Gatekeepers, but according to Laidlaw their democratic impact is so high that they turn into Authority-gatekeeper. Laidlaw exemplified this with the case of Huffington Post, "which discursive significance, has moved it up a level from a micro-IIG to be an authority gatekeeper"[28]. However, some generalisations are feasible, for example Facebook is an Authority Gatekeeper and it is difficult to foresee this changing[29].

Applying these concepts to the scope of this paper, which is Participative Networked Platforms it can be concluded that service providers as Facebook, would be "Authority Gatekeepers". These entities are "intermediaries that have become household names and the functions they serve have become iconic representations of Web"[30]. For instance, LinkedIn and professional networking, YouTube, Wikipedia and general knowledge, Twitter and microblogging among others.[31] These entities have legal and economic machinery and above all, they are visible[32]. For this reason, regulators turn their eyes to them when dealing with liability how will be explained in the next section.

Users, on the other hand are individuals or companies who decide to use online spaces of expression. These are "Micro-Gatekeepers" for instance "the administrator sites such as application and content moderators, and network administrators"[33]. They are not always visible. Authors of the content are at the beginning of the chain and are difficult to identify and therefore difficult to control[34].

---

[27] Bracha and Pasquale, above n 18, at 1162

[28] Laidlaw, above n 2, at 62.

[29] "Some of them started out in small capacities with no obligations and then meteorically shot to the level of authority gatekeeper attracting human rights obligations such as Facebook" : Laidlaw, above n 2, at 60.

[30] See Corey Omer "Intermediary Liability For Harmful Speech: Lessons From Abroad"(2014)28HarvJ.L.& Tech. 287 at 294.

[31] At 294.

[32] "traditional media intermediaries, the giant intermediaries are likely to maintain significantly superior salience and exposure, both on and off the Internet.": Bracha and Pasquale, above n 18, at 1160

[33]Laidlaw, above n 2, at 60.

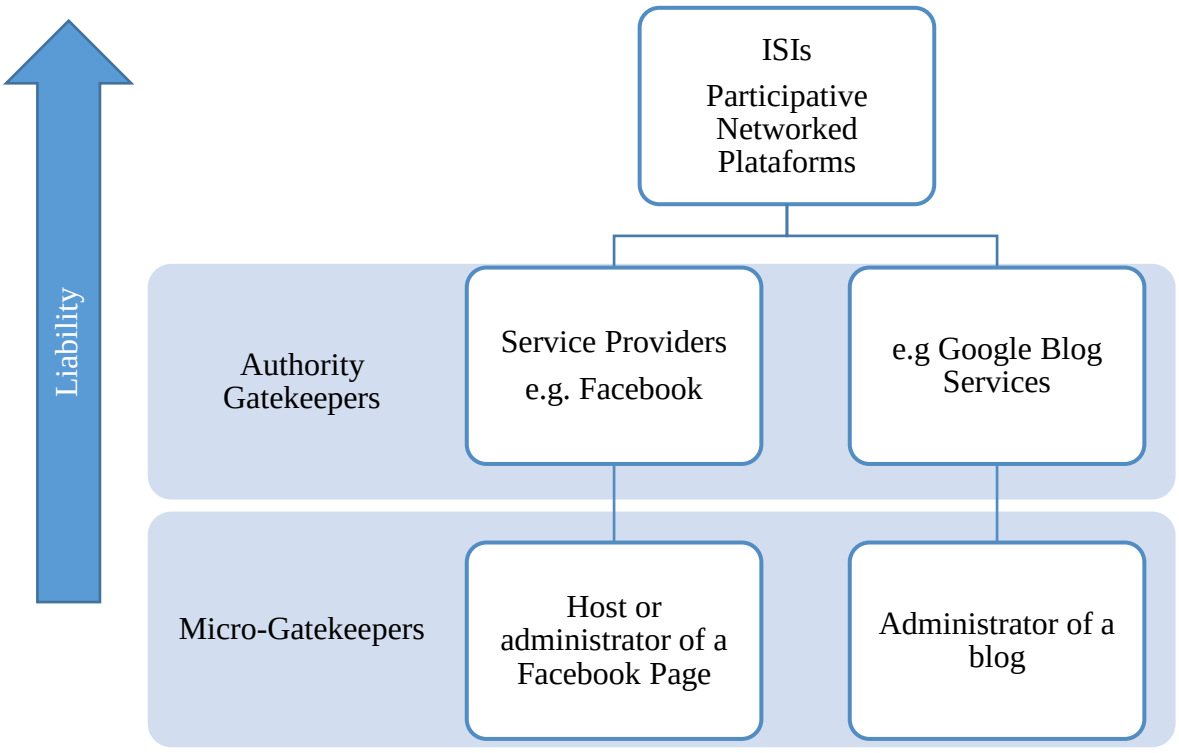
[34] At 60.

Thanks to decentralization of the Internet, everybody with basic knowledge of computer usage, can spread content online. In The United States alone, "every minute YouTube user's upload 100 hours of new video, 25 Instagram users share over 41,000 new photos, Twitter users tweet over 347,000 times, and Facebook users update 293,000 statuses"[35]. This paradigm is troublesome to government and regulators who are unable to penalize the offender in a sea of anonymity.

III Liability of Gatekeepers: Participative Networked Platforms.

This section deals with liability of Authority Gatekeepers and Micro-Gatekeepers, specifically within the category of Participative Networked Platforms. As is seen from the next diagram.

Diagram 6: Layers of gatekeepers applied specifically to Participative Networked Platforms



[35] Omer, above n 30, at 298.

When liability is discussed the above taxonomic discussion gains importance. The responsibility of an Authority Gatekeeper such as Twitter, should not be equitable to the liability of the Micro-gatekeeper as a Facebook Page Host although both of them are ISIs. The proposal of this paper is that to construct an effective ISIs' liability framework, legal sources should take into account the digital reality, by differencing Authority gatekeeper from Micro-Gatekeepers. At this point it is necessary to emphasize, that the heart of the matter when dealing with liability of ISIs is detect who is responsible for the harmful content? As summarized by Professor Susan Corbett:

> Clearly an individual who posts defamatory material online is liable as a publisher; but should an online intermediary such as an internet service provider (ISP), the owner of a blog or website, or a search engine provider, who has facilitated the original posting or its further dissemination, also be liable?[36].

ISIs' liability with its complex chain of communication has been dealt with differently in New Zealand as appose to Europe. This will be explored further in this section.

A Legislation: The Vertical and Horizontal Approach (Europe and New Zealand)

There are two legislative approaches to ISIs' Liability, Horizontal and Vertical. The horizontal approach is applied in Europe[37] through the E-commerce Directive[38]. This approach differentiates between the classes and functions of ISIs for the purpose of limitation of liability"[39] and addresses all the issues in a single piece of legislation. The E-Commerce Directive regime is described in detail below. It should be noted that in recent years the European Commission engaged in consultation with the public on reform to the

---

[36] Susan Corbett "Search Engines and the Automated Process: Is a Search Engine Provider 'a Publisher' of Defamatory Material?" (2014) 20 NZBLQ 200 Retrievable from <http://ssrn.com/abstract=2461499 or http://dx.doi.org/10.2139/ssrn.2461499>.

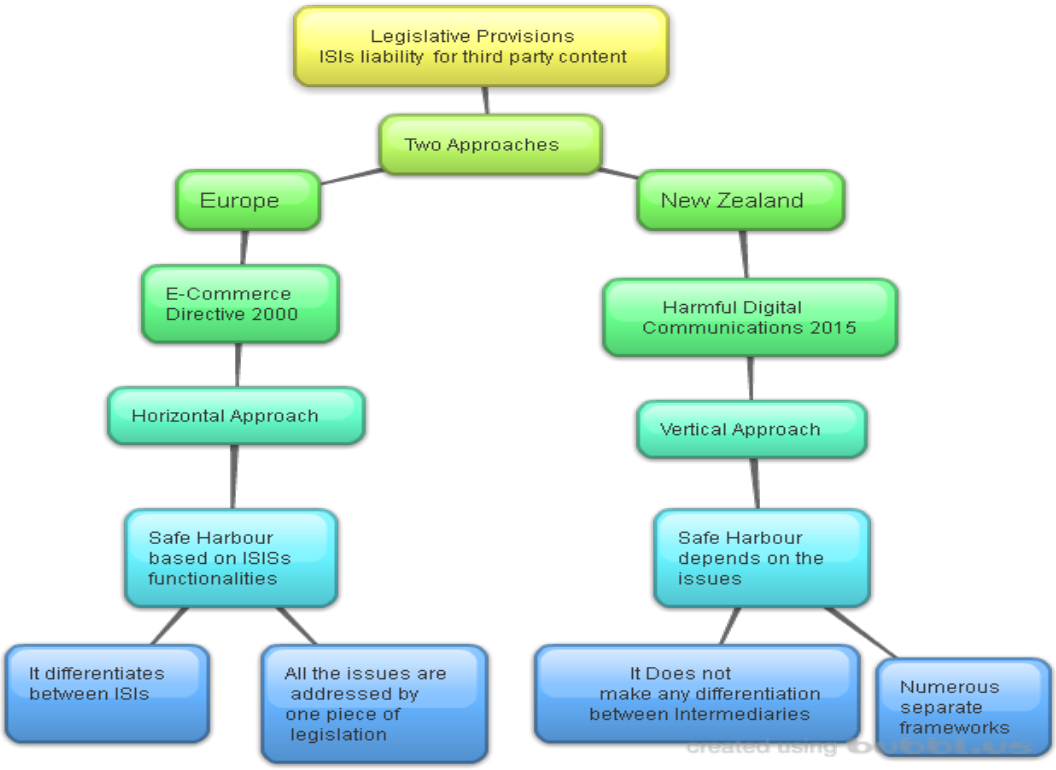
[37] Lilian Edwards "Role and responsibility of the internet intermediaries in the field of copyright and related rights" (Presented at conference in June 2011 before governmental and Industry Representatives, Commissioned by World Intellectual Property Organization, Geneva, 2011) at 7 Retrievable from <http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf >.

[38] Directive 2000/31/EC on Certain legal aspects of information society services in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178, art [12-15].

[39] Jyoti Panday "Comparative Study Of Intermediary Liability Regimes Chile, Canada, India, South Korea, UK and USA in support of the Manila Principles On Intermediary Liability"(1 July 2015) Manila Principles <www.Manilaprinciples.org> at 10.

Directive including arts 12 to 15[40] . On the other hand, the vertical approach "lays down rules for special domains (copyright, protection of children, personal data, counterfeiting, domain names, online gambling among others)"[41]. For example, "US Internet gambling law, the Defamation Act 1996, and the United States and its Digital Millennium Copyright Act of 1998"[42]. In the case of New Zealand, The Harmful Digital Communications Act refers to separate frameworks for matters different from harmful communication (e.g. Copyrights issues are remitted to the Copyright Act 1994)[43]. This approach does not differentiate between types of ISIs[44]. The next diagram illustrates the basic differences.

Diagram 7: Legislative Approaches to ISIs' Liability



[40] See "Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC)", closed November 5 2010, <http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.>

[41] Edwards, above n 37, at 7.

[42] See At 7.

[43] The Harmful Digital Communications Act 2015, s 25 (4).

[44] See Pablo Asbo Baistrocchit "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce" (2002) 19 SantaClaraComputer&HighTechLJ 111 at 117.

As seen from Diagram 7, both of these approaches provide Safe harbour for ISIs. Before going further with each jurisdictional approach it is necessary to establish what "safe harbour " means in the context of ISIs' liability.

1 Safe harbours in legislations.

This system is "a legally safe place that is given to Internet intermediaries meaning that provided their actions follow carefully the procedure, they will not be liable for user actions"[45]. This immunity from liability, under certain restrictions, is a good strategic development which supports the emergence of innovative services and freedom of expression[46]. In the United States for example, the Communications Decency Act Section 230(c) (2) was one of the first legislative bills around the world in recognizing this system. It set out that Intermediaries cannot be held liable for self-policing, restricting access to, or providing others the technical means to restrict access to material considered objectionable[47]. Below this paper explains the legislative approach to ISIs' liability and safe harbour systems in each jurisdiction.

2 Europe Legislation.

(a)The Online Conduct Code.

After recent terrorists attacks in Brussels,[48] the European Union called on all the Authority Gatekeepers, Facebook, Microsoft*, Twitter and YouTube to collaborate to deter Hateful speech[49]. By signing an "Online Conduct Code" these companies show their support to the European Commission and EU Member States for "the challenge of ensuring that online platforms do not offer opportunities for illegal online hate speech"[50]. One of the conducts that Authority Gatekeepers agreed to by signing the Online Conduct Code is "to review the

[45] Zingales, above n 9.

[46] See Article 19 "Internet intermediaries: Dilemma of Liability" (2013) < www.article19.org>

[47] Communication Decency Act, 47 U.S.C. § 230(c) (1996).

[48] "Three men walked into the departure lounge at Brussels' Zaventem airport shortly after 8.30am local time – 7.30am in London. The two blasts ripped through the building, leaving at 11 people dead and dozens injured. 10 are in a critical condition (…) Islamic State of Iraq and the Levant (Isil) has already claimed responsibility for the attacks" : Peter Foster "What happened in Brussels?" *The Telegraph UK* (Online Ed, London, 22 March 2016) retrievable from < http://www.telegraph.co.uk/news>.

[49] Commission Press Release "European Commission and IT Companies announce Code of Conduct on Illegal online hate speech" IP/16/1937 (31 May 2016).

[50] Commission of The European Communities *Code of Conduct on Countering Illegal Hate Speech Online* (2016) Retrievable from <http://ec.europa.eu >.

majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary"[51]. Additionally, the IT Companies pledge themselves "to educate and raise awareness with their users about the types of content not permitted under their rules and community guidelines". By creating this code, the European Communities implicitly recognized the importance of Authority Gate-keepers as important stakeholders in society. This is because these companies have the technological tools to utilise different, traditionally government, powers in the online world such as controlling an individual's speech.

Some communities are already speaking out against the code. One of the major aspects of disagreement relates to the fact that effectively the Code recognises, it is companies who are *taking the lead* on deterring illegal hate speech online. But "in a society based on the rule of law, private companies should not take the lead in law enforcement otherwise this leads to arbitrary censorship of our communications"[52]. On a positive note, the Code engages Authority Gatekeepers to prevent harmful communications by educating their users. This is not a disempowerment of the government but more of a collaborative effort. This feature is a very Avant-garde approach because it places responsibilities on the agents who are capable to assume them, recognising the reality of technology today.

(b) The E-commerce Directive: Passive reactive Safe harbour s?

Europe holds a horizontal approach which does differentiate between ISIs. It has one piece of legislation to address all the possible issues independent of the exact subject. Article 12 establishes the "safe harbour" for ISIs by dividing these entities into three types according to their activity: (i) mere conduit[53], (ii) caching[54], and (iii) hosting[55]. ISIs "acting as mere conduits are protected from liability potentially arising from transmitted content, provided that they are only passively involved in the transmission". Caching is the temporary storage of information, "while hosting providers store third-party content for a potentially indefinite period of time"[56].

---

[51] At 2.

[52] Joe McNamee "Guide to the Code of Conduct on Hate Speech" (3 June 2016) EDRi <https://edri.org>

[53] Directive 2000/31/EC, above n 38, art 12.

[54] Art 13

[55] Art 14

[56] Mlynar Vojtech "A Storm in ISP Safe Harbour Provisions: The Shift From Requiring Passive-Reactive to Active-Preventative Behavior and Back" (2014) 19 IntellPropLBull 1 at 7.

The “safe harbour” for every ISI is different but they have common ground. The common ground is the notion of “actual knowledge” of the offensive material. ISIs are protected from liability in two circumstances: The ISI “does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity is apparent"[57]; or the ISI “upon obtaining such knowledge or awareness, acts expeditiously to remove or to disrupt access of the information”[58].The ISI must not have actual knowledge of illegal activity or infringing information otherwise it would be liable. Additionally, under the Directive ISIs “cannot be required to perform general monitoring of content passing through their systems. Instead, they typically follow a notice-and takedown procedure when dealing with infringing activities”[59]. This illustrates the EU's intention for ISIs “to remain passive-reactive. As long as intermediaries act passively and neutrally by automatically caching data without monitoring its content”[60].

(c) Human Rights Framework: European Convention for the Protection of Human Rights and Fundamental Freedoms, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

In recent case of *Barbulescu v Romania* addressed by the European Court of Human Rights[61] the dissenting Judge Pablo Pinto de Albuquerque established that “user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression”. He also established that:

> States have a positive obligation to promote and facilitate universal Internet access, including the creation of the infrastructure necessary for Internet connectivity. In the case of private communications on the Internet, the obligation to promote freedom of expression is coupled with the obligation to protect the right to respect for private life[62].

ISIs and more specifically participative networked Platforms are an important tool of internet connectivity, therefore their use is covered by this framework. In other words,

---

[57] Art 14.

[58] Art 12 ; *see also* Benoît Frydman and Isabelle Rorive “Regulating Internet Content Through Intermediaries in Europe and the USA, Zeitschrift fur Rechtssoziologie” (2002) 23 HEFT41

[59] Vojtech, above n 56, at 8.

[60] At 12.

[61] *Bărbulescu v. Romania* (2016)13 EHRR 29 (Section IV, ECHR) at 28 per Judge Pinto de Albuquerque dissenting at [3].

[62] At [3]

individuals use Participative Networked Platforms because they have the right of freedom of expression. First of all, Article 19 of the Universal Declaration of Human Rights (UDHR)[63] guarantees the right to freedom of expression in the following terms: "this right includes the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers[64].This is complimented by the European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 10 establishes that "this Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises"[65]. The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the UDHR[66]. Article 19 of the ICCPR[67] states that: "(…) this right shall include freedom to seek, receive and impart information and ideas of all kinds, (…) in the form of art or through any other media of his choice"[68].

Therefore, Freedom of expression comprehends others dimensions of speech. Not only the right of individuals to express themselves but also to access an online world of information. ISIs offer the technological tools and platforms to individuals to achieve these purposes. The OECD recognised the significance of Participative networked platforms by establishing that:

> Never before have had so many people introduced so many kinds of content, on such a broad scale, and potentially with such wide-ranging impacts. Changes in the way users produce, distribute, access and re-use information, knowledge and entertainment are likely to continue to have structural impacts on the cultural, social and political spheres.[69]

The recognition provided by the above statement illustrates a true realization of Freedom of expression that the ISIs now provide. The council of the OECD recognised that "appropriate limitation of liability for Internet intermediaries plays a fundamental role in

---

[63] *Universal Declaration of Human Rights* GA Res 217A, III A/Rcs/801 (1948), art 19.

[64] Art 19.

[65] European Convention on Human Rights 213 UNTS 221 (opened for signature 4 November 1950, entered into force 3 September 1953) art 10.

[66] Article 19, above n 46.

[67] International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976) [the ICCPR], art 19.

[68] Art 19.

[69] OECD, above n 10, At 43.

promoting innovation and creativity, the tree flow of information"[70], in other words true freedom of expression. In fact, in response ISIs have built their defence from third party content liability. The section B of this title analyses one of the most iconic cases regarding Participative Networked Platforms (*Delfi AS v Estonia[71])* that illustrates the use of freedom of expression as ISIs' defence from Liability.

3 New Zealand Legislation.

New Zealand applies a vertical approach. As in the United States, there is a separate piece of legislation to address every issue that could arise from ISIs' liability. The scheme is constructed according to the rights which are affected (e.g. copyrights) rather than in the condition of the ISIs. This vertical approach is visible in the Harmful Digital Communications Act 2015[72] when it establishes that nothing in the ISIs' liability section (s24 and s25) affects the following provisions: "section 211 of the Criminal Procedure Act 2011; or section 19 of the Bail Act 2000; or copyright liability, or any proceedings, under the Copyright Act 1994". [73]

(a)Harmful Digital Communication Act: The confusion between Authority Gatekeepers and Micro- Gatekeepers.

The Harmful Digital Communication Act was enacted in 2015 and was intended to sufficiently comprehend Participative Networked Platforms. For instance, the Law Commission set out that Harmful communications as a concept not only applies:

> (…) to one-to-one communication but more broadly to the range of digital publishing which occurs in cyberspace. This includes the uploading of user generated content (audio-visual, pictures or text) on websites and platforms such as YouTube and Facebook, and the use of micro-blogging sites like Twitter to disseminate information and opinions.[74]

---

[70] "We recognised that the Internet allows people to give voice to their democratic aspirations, and any policy-making associated with it must promote openness and be grounded in respect for human rights and the rule of law": Organisation for Economic Cooperation and Development *Recommendation of the Council on Principles for Internet Policy Making* (2011) Retrievable from < http://acts.oecd.org> .

[71] *Delfi AS v Estonia* (64569/09) Grand Chamber ECHR 16 June 15.

[72] The Harmful Digital Communications Act 2015.

[73] S 25: Or "any enactment that expressly overrides section 24".

[74] Law Commission, above n 3, at [16].

This legislation do not differentiate between Micro-Gatekeepers and Authority gatekeepers. Actually, all ISIs are grouped into one single concept: The concept of Internet Online Hosts. The Online Hosts are described by the act as "the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user".[75] Therefore, Both micro and Authority Gatekeepers could fall in this description. The consequence of this, is that Micro-Gatekeepers such as Facebook Page Hosts must abide by the same Safe harbour rules as Authority Gatekeepers to benefit from the scheme. As highlighted below, when addressing case law, some Micro-Gatekeepers may be simple citizens and individuals that under this new Act must follow a reasonably complicated safe harbour scheme.

The safe harbour provisions in the HDCA are contained in s24 and 25: "No civil or criminal proceedings may be brought against an online content host in respect of the content complained of (the specific content) if the online content host (a) receives a notice of complaint about the specific content; and (b) complies with subsection 2"[76]. This concept does not include the scenario where the host did not receive a complaint. It begs the question, if a presumption of the intermediaries' lack of knowledge would operate? Either way it appears the spirit of this legislation is that ISIs should not be responsible for third parties content that they did not acknowledge.

What s24 does do is set out that the fact an online content host does not take advantage of the Safe harbour, does not in itself (not taking advantage) create any civil or criminal liability for hosting the specific content. But if the intermediary follows the procedure it would have a "protection", however section s24 does not make it clear what kind of protection is given or define the term "specific content". Does this ambiguity mean that if a user found an entire page offensive it does not classify as "specific content"?

The critical point this paper attempts to make is that law makers did not take into account the differences between ISIs when designing the safe harbour s scheme. Below, Diagram 8 illustrates step by step the procedure that an "online host" has to follow in order to get the benefits from the safe harbour, as is seen from the image this scheme is rather complicated. As pointed out above, the scheme is based on the ISIs actual knowledge of the harmful communication, which is favourable, but the scheme still may be too complex to follow by some Micro-Gatekeepers.

---

[75] The Harmful Digital Communication Act, above n 43, s 4.

[76] S 25.

(i) A practical example of why the safe harbour (s) 25 is not effective to address liability of all type of ISIs: One size does not fit all. The Case of “Vic Deals”.

A Facebook page works by facilitating an online space for users “to share their stories and connect with other people. Like profiles, a page can be customised by publishing stories, hosting events and more”[77]. Users (Any individual) can create a page and invite other users. They can control the content of the page. The tool available for users is called “the Settings tab”[78] which has a lot of control over your page and the way your content appears. Users have general control for Page and Post visibility, for instance “who sees the Page and who can make changes to the Page”[79].

Moving to a prime example, there is a very popular Facebook Page in Wellington New Zealand called “Vic deals”[80]. The Host of this Page would be a Micro-Gatekeeper according to the definitions of Section II in this document. This page “was setup by marine biology student Carl Meyer, who arrived at Victoria University and thought noticeboards around campus were an inefficient way to advertise goods”[81]. This Facebook page has become so popular that by June 2016 it has more than 54,330 participants with the potential to host a very substantial number of post per day. Recently the Police have begun browsing this Facebook page because “it is has become popular for reporting crime, items that have been lost or found, and advertising flats. More dubious posts include people asking for "420" – a codename for marijuana”[82].

---

[77]Facebook “How Do I Create a Page” (2016) Facebook, Inc. retrievable from <www.Facebook.com/help>

[78]Facebook “Administrator tools” (2016) Facebook Inc. Retrievable from < https://www.facebook.com/business/learn/facebook-page-admin-tools>

[79] At 1.

[80] See Vic Deals page retrievable from < https://www.facebook.com/search/top/?q=vic%20deals>

[81] Samantha Whittle "Making a big deal of university students' needs" *Dominion Post* (Online ed, Auckland, April 9 2015) Retrievable from <http://www.stuff.co.nz/dominion-post/capital-life/capital day/67660102/making-a-big-deal-of-university-students-needs.html>.

[82] Tommy Livingston "Police keeping an eye on Vic Deals Facebook group" *Dominion Post* (Online ed, Auckland, January 12 2016) Retrievable from <http://www.stuff.co.nz/dominion-post/news/74458344/police-keeping-an-eye-on-vic-deals-facebook-group>.

The police do not contact the administrator of the Facebook page (Carl Meyer) but it does monitor the website directly. Additionally, Meyer said that occasionally they get inappropriate posts, but these are usually deleted very quickly. “Members are able to report posts they think are inappropriate, which is a helpful feature of Facebook groups."[83]

The above example indicates that Participative Networked Platforms are gaining relevance for authorities due to their impact on society. However, this fact begs the question, should users in democratic society be aware that they are being monitored by authorities in places of expression that are supposed to allow freedom of speech? Returning to the subject of the liability of the host, under the new Harmful Digital Communication Act, Carl Meyer as administrator of this page would not be liable for the illicit activities of users or for third party content in general. Unless users have reported the content to him and he failed to remove it. This is set out in s25 of the Act under the title “Process for obtaining protection against liability for specific content”. The act established that “[n]o civil or criminal proceedings may be brought against an online content host in respect of the content complained of (the specific content)”[84] as long as “the online content host receives a notice of complaint about the specific content”[85] and he proceeds to take it down.

If Meyer does want to gain all the benefits from the safe harbour established in the Harmful Digital Communications Act he should follow a strict procedure as depicted in Diagram 8 below. It must be remembered that the safe harbour as designed in the act is an added help to ISIs looking to protect themselves against liability for third party content, and it is not mandatory. “The fact that an online content host does not take advantage of section 24 does not in itself create any civil or criminal liability for hosting the specific content”.[86]

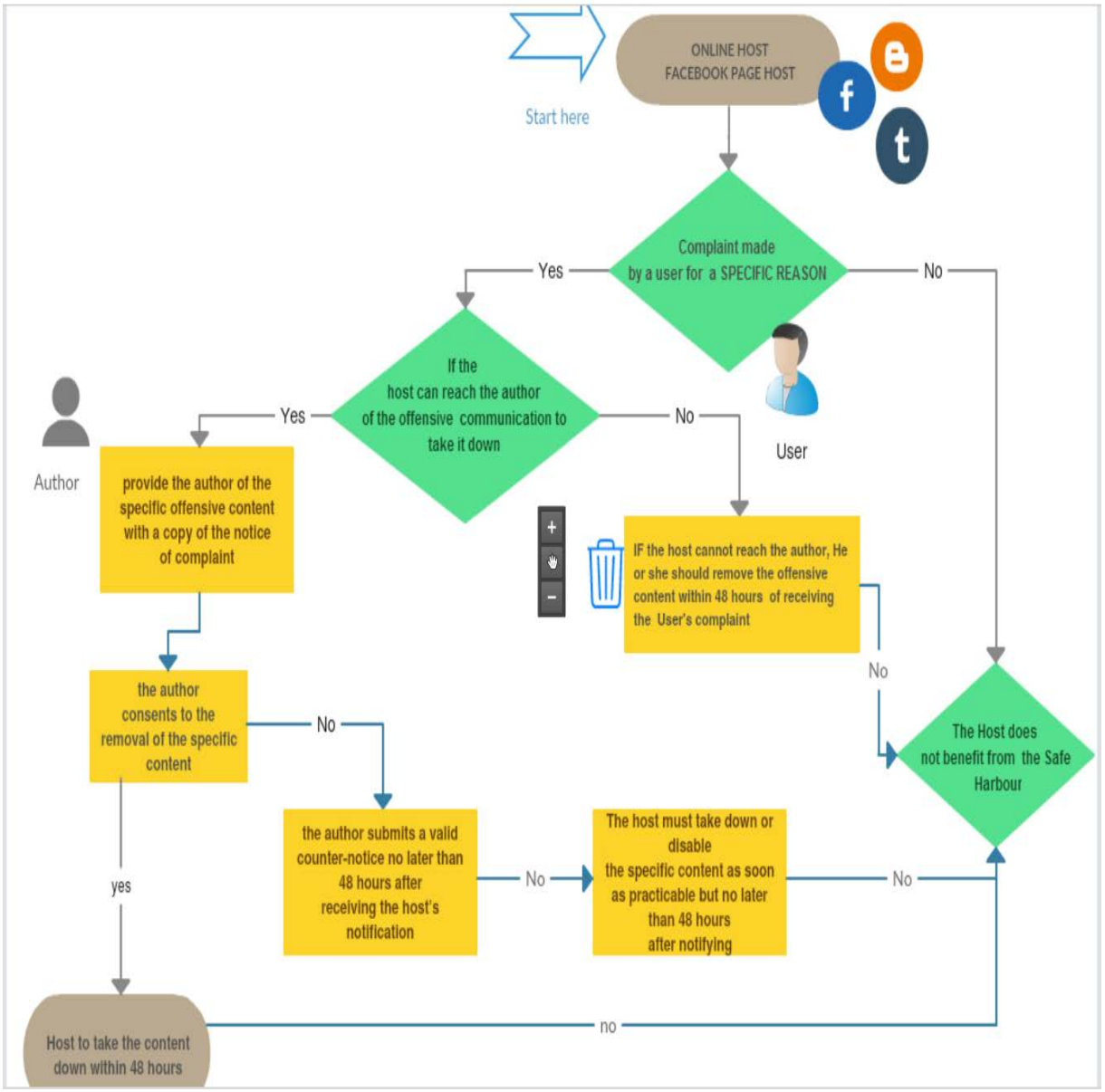
Diagram 8: Safe Harbour, Harmful Digital Communication Act.

[83] At 1.

[84] The Harmful Digital Act, above n 43, S 25.

[85] S 25.

[86] S 23.



As seen from the diagram above, the process to comply with the safe harbour scheme is complex. In cases that are similar to the Vic Deals example, where the host is just an individual with no legal background, the role of the authorities in effectively communicating this procedure is vital. The ideal situation envisaged would be one where Micro-Gatekeepers would have their own scheme. This would include measures that take into account that users are not always as powerful and full of resources as for example the Facebook or LinkedIn corporations. However as stated previously, the Act does not differentiate between online hosts, demonstrating that legal sources do not take into consideration the technological reality when enacting laws.

There are of course positive aspects of this legislation. There is the obligation of the host to ask the authors of the content to remove it themselves and even gives them an opportunity to express why they consider that it should not be removed[87]. For this the act gives an explicit length of time, 48 hours after the host received the complaint by the offended. This results in a reduction of the legal uncertainty during the Safe harbour process (e.g. How many days to take down the content among other issues), and secondly the safe guard of Freedom of Expression, because it provides the author of the speech the opportunity to defend his or her ideas. Recognising that simply because content offends someone does not make it *ipso facto* a Harmful Communication[88].

B ***Case Law: The cost of not differentiating Micro-Gatekeepers from Authority Gatekeepers.***

This section depicts the most iconic cases involving Participative Networked Platforms. As mentioned above, case law in New Zealand and Europe has failed to understand the true dynamics behind micro-gatekeeping. This has resulted in these entities being attributed obligations that may result in a freedom of expression restriction. The source of this failure is that when it comes to online harmful communications, legal sources turn to defamation frameworks in other to resolve the liability of ISIs. Looking at it in this light would mean considering harmful communications to be "publications" making ISIs publishers, thus liable for the author's message. The courts in both New Zealand and Europe have tried to resolve issues that arise from the Internet by applying analogies out of date which leads to legal inaccuracy and uncertainty.

---

[87] S 24 [(b)-(d)].

[88] "Not all harms arising from communications are proscribed by law. Criminal law has typically been concerned with protecting citizens from harmful communication which invokes fear for physical consequences, either personal or proprietary, or which are obscene or harmful to children. Civil law, in the past, also typically shied away from providing remedies for emotional harm as such. However, as demonstrated later, in both civil and criminal spheres the law has been moving towards recognition of, and protection from, emotional harm." Law Commission, above n 3, at [18].

1 Europe Case law.

(a) Delfi v Estonia.

The landmark European Court of Human Rights judgment in *Delfi AS v Estonia*[89] is an elevated standard of responsibility which was imposed on an online news portal for third parties content. In this case "The applicant is the owner of Delfi, an Internet news portal that publishes up to 330 news articles a day at the time of the lodging of the application"[90]. Some opinions would view Delfi as an Authority Gatekeeper due to its democratic impact and its economic and legal machinery. However there is a notable difference in that Delfi does not own the platform itself, like the "website domain" how Google does for example.

"On the 24th of January 2006 an article with the title "SLK Destroyed Planned Ice Road" was published"[91] on Delfi's news portal. The article suggested that AS Saaremaa Laevakompanii (Saaremaa Shipping Company) made it impossible to use several ice roads in Estonia[92]. Delfi opened a forum just below the article for readers to comment and give personal opinions about this report. An individual identified by the Court as 'L" was member of the board of the above mentioned company. Some of the comments that users posted on Delfi's page were personal comments about "L" with a particularly offensive tone[93]. On 9 March 2006 L's lawyers requested Delfi to remove the comments and claimed approximately 32,000 euros in compensation for non-pecuniary damages. This was on the basis of a believed breach of Article 8 of the Convention[94]. Delfi complained that holding it liable for the comments posted by the readers of its Internet news portal infringed its freedom of expression as provided for in Article 10 of the European Convention for the Protection of Human Rights[95]. Delfi argued that "it was sufficient for a host to expeditiously remove third-party content as soon as it became aware of its illegal nature"[96].

---

[89] *Delfi AS v Estonia*, above n 71.

[90] At [11].

[91] At [16].

[92] At [16]

[93] "Wonder whether [L.] won't be knocked down in Saaremaa? screwing one's own folk like that"; "[little L.] go and drown yourself": At [18]

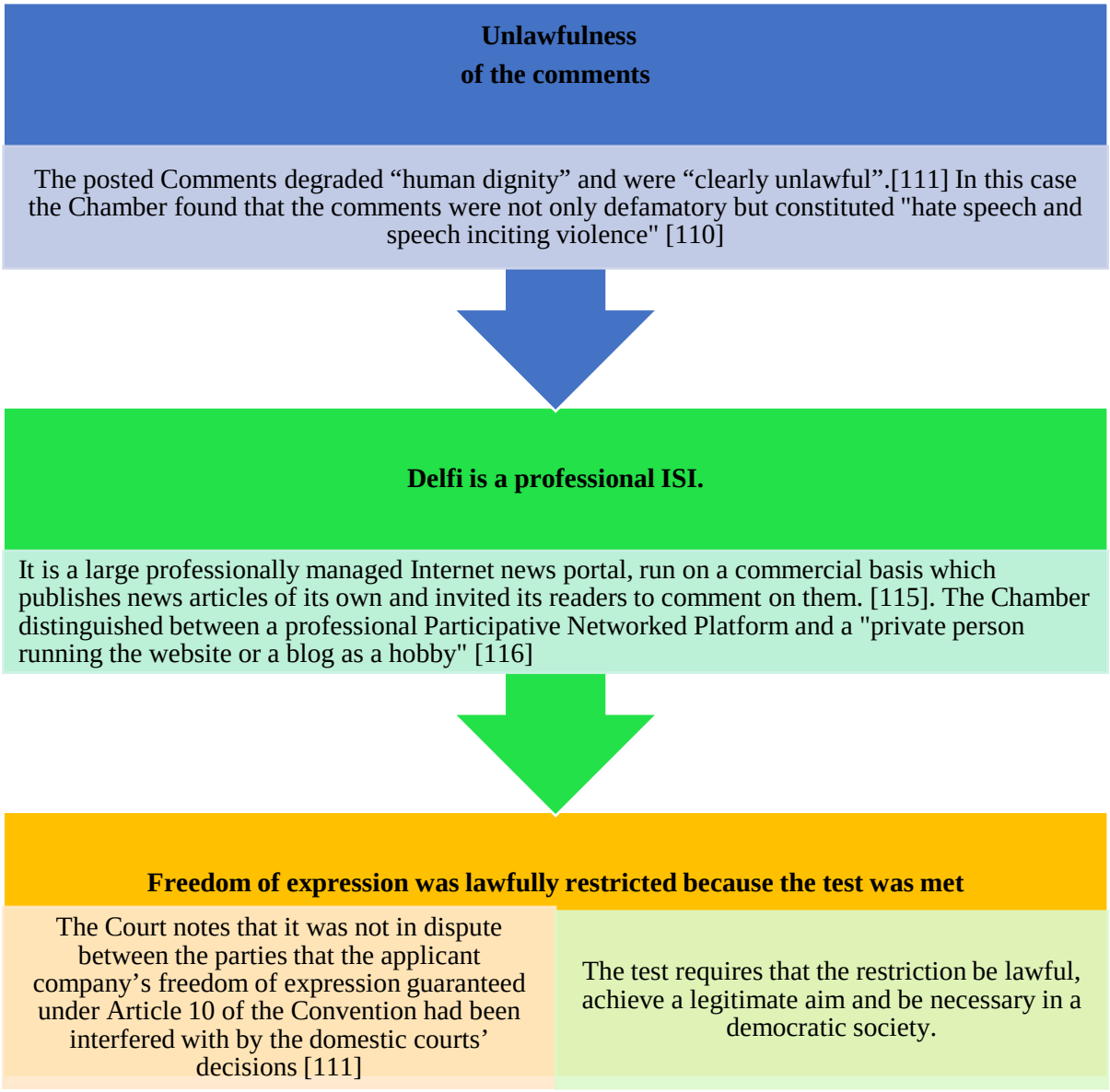
[94] European Convention on Human Rights, above n 65, Article 8: "Right to respect for private and family life 1. Everyone has the right to respect for his private and family life, his home and his correspondence".

[95] At [59]

[96] At [67]

The Grand Chamber (European Court of Human Rights) noted the novelty of the case, being the "first case in which the Court has been called upon to examine a complaint of this type in an evolving field of technological innovation"[97]. The court also considered that because of the particular nature of the internet an internet news portal may differ to some degree from those of a traditional publisher, as regards third-party content[98]. However by using the following reasoning, the Chamber found that Delfi was liable for defamation:

Diagram 9: Liability of an Online News Portal for third parties comments Delfi As v Estonia.



[97] At [111]

[98] At [113]

In several respects this decision set a deeply concerning precedent for freedom of expression. “It also displays a worrying lack of understanding of the issues surrounding intermediary liability and the way in which the Internet works”[99]. It restricts freedom of expression because it imposes on Participative Networked Platforms Hosts the active role of monitoring and taking down if necessary any content on the basis of preventing hateful speech. The foreseeable consequence of this case is that news portals will likely remove completely their comment spaces because of the fear of facing liability for third parties content. If that happens users will lose a valuable way of engaging in matters of public debate and it will lead to an increase in private censorship.

2 New Zealand Case Law.

(b) O’Brian v Brown[100].

The case *O’Brian v Brown* addressed by the “District Court found that a publication on the internet is a publication for the purposes of the New Zealand Defamation Act”[101], meaning that the intermediaries involved may be publishers. A fundamental principle of defamation law is that liability for publishing prima facie applies to any entity which has played a part in disseminating defamatory material[102], therefore Micro-Gatekeepers would be liable as publishers.

(c) Wishart v Murray[103].

In this case, Courtney J explained that they are not passive instruments or mere conduits of content posted on their Facebook page. They are the publishers of postings made by users in two circumstances:

---

[99] Article19 "European Court strikes serious blow to free speech online" (2015) Article19 <www.article19.org>.

[100] *O’Brien v Brown* [2001] DCR 1065.

[101] Corbett, above n 36, at 1.

[102] At 2.

[103] “The facts of the case were that the plaintiff Ian Wishart a well-known journalist and writer wrote a book about the story of Macsyna King accused of murdering her new born twins. Although the father Chris Kahui, was acquitted of their murder he suggested that the babies' mother, had inflicted the fatal injuries. Mr Murray, created a Facebook page called "Boycott the Macsyna King Book" where individuals uploaded comments expressing their disagreements with the book. Regarding liability of Facebook Pages Hosts for third parties content”: *Wishart v Murray* [2013] NZHC 540, [2013] 3 NZLR 246.

a. The "Actually know Test"[104] If the Facebook Page Host knows of the defamatory statement and fails to remove it within a reasonable time in circumstances that give rise to an inference then they are therefore responsible for the content.
b. The "Ought to know test" a request by the person affected is not necessary. The Facebook Page Host does not know of the defamatory posting but ought to have, in the circumstances, to know that postings are being made that are likely to be defamatory.

During this case various analogies were applied by Courney J in order to establish the liability regime of a Facebook Page Host, the one which she applied to reach the conclusion of Mr Murray's liability was the analogy of the vendor: Courtney J applied an analogy based on *Emmens v Pottle*[105]"This case concerned a claim for defamation against news vendors who had sold copies of a magazine containing a defamatory statement about the appellant"[106] Courtney J applied it to conclude that "the absence of actual knowledge does not prevent a person who, prima facie, publishes a defamatory statement from being liable. Hence Mr Murray (seen as a vendor) "ought to know" about the offensive third party comments and was liable for it.

(d) Murray v Wishart[107].

In the appeal, NZCA did not agree and concluded that *Emmens v Pottle*[108] was not an appropriate analogy for the Host of the Facebook page. The NZCA analyses:

> The news vendor is a publisher only because of the role taken in distributing the primary vehicle of publication, the newspaper itself. This contrasts with the host of a Facebook page which is providing the actual medium of publication, and whose role in the publication is completed before publication occurs.[109]

---

[104] This test were baptized in the appeal by the NZCA in *Murray v Wishart* [2014] NZLR 722 at *[98]*.
[105] Emmens v Pottle (1885) 16 QBD 354 (CA).
[106] *Murray v Wishart*, above n 104, at [98].
[107] at [98].
[108] *Emmens v Pottle* above 105.
[109] Additionally the NZCA held that *Emmens v Pottle* "is authority for the proposition that a news vendor who does not know of the defamatory statement in a paper he or she sells is a publisher, and must rely on the innocent dissemination defence to avoid liability. So a decision that the host of a Facebook page could be liable for statements appearing on the page of which he or she is not aware would not necessarily be an unprecedented situation (…) the news vendor is a publisher only because of the role taken in distributing the

NZCA concluded that the 'actual knowledge' test should to be employed in that particular situation.[110] This means that a Facebook page host would be liable only if it had 'actual knowledge' of the offensive content and fails to remove these posts within a reasonable time[111].

The actual knowledge test is aligned with the introduction of the HDCA - section 24 which imposes liability for an internet host who has actual knowledge of defamatory material and fails to remove it. The HDCA does not differentiate between micro-keepers and Macro-Keepers, therefore is feasible to say that s24 is applicable for a host of Facebook pages or administrators of a website among others. The 'actual knowledge' test is also consistent with the protection of freedom of expression because hosts of pages will be less pressured to take down content for the fear of legal consequences.

(e) Karam v Parker[112]

Joe Karam, sued Mr Parker and a Mr Purkiss for numerous statements published online about the trial of David Bain. This claim arose from comments on a Facebook page, on a website called 'Counterspin', Trademe and Youtube. Mr Parker denied being the publisher of statements by third parties, relying on the defence of innocent dissemination under s 21 of the Defamation Act 1992 applicable to Vendors. Interestingly Courtney J who applied the vendor's analogy in *Wishart v Murray* held in *Karam v Parker* that those who host Facebook pages or similar sites are to be regarded as publishers of postings made by others in two circumstances. She decided to apply first the test of "the actual knowledge" of harmful content by quoting herself when explaining this test. "The first is if they know of the defamatory material and do not remove it within a reasonable time in circumstances that give rise to an inference that they are taking responsibility for it".

The different outcome in the two cases with similar factual aspects creates an uncertainty about the liability system applicable to Micro-Gatekeepers. Moreover, if the Facebook Page Host is not a vendor, the exception of liability for innocent dissemination does not apply. It is urgent that legal sources reach unanimity on this regard. There is also the question of the

---

primary vehicle of publication, the newspaper itself. This contrasts with the host of a Facebook page which is providing the actual medium of publication": *Murray v Wishart* , above n 104, at [128].

[110] *Murray v Wishart*, above n 104, [144]

[111] *Murray v Wishart*, above n 104, [145-147]

[112] *Karam v Parker* [2014] NZHC 737

high award to the plaintiff in this case ($530,000)[113]. Leaving aside the reproachable conduct of Mr Parker, the question that arises is if this amount of money is a proportionate sanction for administrating an opinion group over the Internet. This kind of punitive outcome is very detrimental for the freedom of speech.

IV Conclusions

The collaboration of Authority Gatekeepers is essential for governments to deter harmful digital communications on the Internet. This is because authors of the speech are not easily detectable in cyber space and the traditional liability system is no longer effective in this context. It is understandable then that legal sources have turned their attention to regulate noticeable gatekeepers on the Internet (e.g. Facebook, Twitter, YouTube) for third party content as they are the only visible contributors to exercise control over. However, in order to safeguard freedom of expression rigid systems of liability for these intermediaries should be formulated.

This paper explored two important frameworks for their contribution to Internet Intermediaries liability. The Harmful Digital Act 2015 in New Zealand, has taken a step forward towards recognising the Safe harbour for online hosts. By enacting this act the legislator is acknowledging Safe harbours as indispensable to reach a balance between freedom of expression and other rights on the Internet. Having said that, The E-commerce Directive in Europe which recognizes limitations to ISIs' liability by differentiating between these entities is perhaps a greater step towards more accurate legislation.

Nevertheless, there is a lot of work to do regarding the conceptual foundation of both legislations because as explained, the difference between Intermediaries on the internet is far from being moot and so far neither of them makes an entirely accurate differentiation. The distinction between Authority gatekeepers and Micro-Gatekeepers must be implemented in any framework that deals with the liability of an online host. Authority gatekeepers are big corporations that have all the legal and economic machinery to address their responsibility for third parties communications, whereas Micro-Gatekeepers could be any individual that decides to open a space for sharing opinions.

[113]Jared Savage "Karam awarded $535,000 over defamation" *The New Zealand Herald* (Online ed, Auckland, 17 april 2014) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11239379>

This categorization should not be only be implemented in legislation but in case law also. As studied in cases like *Delfi v Estonia* the Court failed to apply correctly the E-commerce directive and understand the role of Participative Networked Platforms as gatekeepers to the exercise of freedom of expression. The Court also emphasizes continually that the applicant company was a newspapers operator and a professional ISI rather than, for example, an individual blogger moderating a blog for a hobby. In the end the Court sent two contradictory messages in the sense that one is a progress and the second is a misinterpretation. The first that in order to protect freedom of expression and others rights the differentiations between ISIs should be made. And the second, that a newspapers platform would be *prima facie* liable if they do not remove hateful speech. This last one, basically overrides the provisions in the E-commerce directive.

Cases like *Wishart v Murray* prove that legal sources are not yet prepared to recognize Micro-Gatekeepers as a new special agent in the chain of communication. Possibly even more concerning is the fact that in the case of *Karam v Parker* the host of a Facebook page was liable to pay $530,000 for his opinion on the Internet. This may send the wrong message to society that it is better to stay away from spaces of discussion on the Internet and could also lead to undesirable censorship. Lastly, it is pertinent to cite Stephen Todd who wrote that "…as regards the internet, a uniform approach remains elusive … It would appear that presumptions do not work well in relation to the Internet and the factual matrix and policy concerns will feature strongly in these cases"[114] .

[114] Stephen Todd *The Law of Torts in New Zealand* (6th ed, Brookers, Wellington, 2013) at [16.5.02].

V BIBLIOGRAPHY.

A PRIMARY SOURCES

B Legislation

1 New Zealand

Bill of Rights Act 1990.
Defamation Act 1992
Harmful Digital Communication 2015.

2. *United States*
Communications Decency Act 47 USC § 230.
Digital Millennium Copyright Act 17 USC § 512.

3. Europe

Commission of The European Communities *Code of Conduct on Countering Illegal Hate Speech Online* (2016) Retrievable from <http://ec.europa.eu >.
Directive 2000/31/EC on E-commerce [2000] OJ L 178
European Convention on Human Rights 213 UNTS 221 (opened for signature 4 November 1950, entered into force 3 September 1953) .
International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976).
Universal Declaration of Human Rights GA Res 217A, III A/Rcs/801 (1948).

C Cases

3 New Zealand

A v Google New Zealand Ltd HC Auckland CIV-2011-404-2780, 12 September 2012.

A v Internet Company of New Zealand [2009] ERNZ 1.

Karam v Parker [2014] NZHC 737.

O'Brien v Brown [2001] DCR 1065.

Sadiq v Baycorp (NZ) Ltd HC Auckland CIV 2007-404-6421, 31 March 2008.

Wishart v Murray [2013] NZHC 540.

Murray v Wishart [2014] NZLR 722.

4 Canada.

Emmens v Pottle (1885) 16 QBD 354 (CA).

3. European Union

Bărbulescu v. Romania (2016) 13 EHRR 29 (Section IV, ECHR).

Delfi AS v Estonia (64569/09) Grand Chamber ECHR (16 June 15).

4. United Kingdom

Godfrey v Demon Internet Ltd [2001] QB 201, [1999] 4 ER 342 (QB).

Tamiz v Google Inc [2013] 1 WLR 2151 (CA).

Byrne v Deane [1937] 1 KB 818.

D Government and Official Materials

5 New Zealand.

Law Commission *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (NZLC SP23534, 2012).

Ministry of Justice *Harmful Digital Communications Bill – Departmental Report for the Justice and Electoral Committee* (13 April 2014).

6 European Union.

Commission of The European Communities *Code of conduct on countering Illegal hate speech online* (2016) .

"Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC)", closed November 5 2010, <http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.>

7 Multilateral instruments.

Organisation for Economic Cooperation and Development *Recommendation of the Council on Principles for Internet Policy Making* (2011).

B SECONDARY SOURCES.

E Books.

Matthew Collins *The Law of Defamation and the Internet* (3rd ed, Oxford University Press, New York, 2011).
Stephen Todd *The Law of Torts in New Zealand* (6th ed, Brookers, Wellington, 2013) at [16.5.02].

F Journals

Pablo Asbo Baistrocchit "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce" (2002) 19 SantaClaraComputer&HighTechLJ 111.

Blake E Ashforth, Glen E Kreiner and Mel Fugate "All in a day's work: Boundaries and micro role transitions"(2000) 25(3) ASJC 472.

Jack Balkin "Digital speech and democratic culture: A theory of freedom of expression for the information society" (2004) 79 NYULRev 1.

Karine Barzilai-Nahon "Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control" (2008) 59 JAmSocInfSci 1493.

Oren Bracha and Frank A Pasquale "Federal search commission? Access, fairness and accountability in the law of search." (2008) 93 CornellLRev 1149.

Jürgen Habermas "Political communication in media society: Does democracy still enjoy an epistemic dimension? the impact of normative theory on empirical research" (2006) 16 CT 411.

Lesiak Malgorzata "A Comparative Analysis of the Liability of Internet Service Providers in the Context of Copyright Infringement in the US, European Union and Poland" (2015) 3 Mujlt 219.

Etienne Montero and Quentin Van Enis "Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle?" (2011) 27 CLSRev 21.

Bailey Rishab "Censoring the Internet: The New Intermediary Guidelines" (2012) Febrary 4 EconPolitWkly 1.

MlynarVojtech "A Storm in ISP Safe Harbor Provisions: The Shift From Requiring Passive-Reactive to Active-Preventative Behavior and Back" (2014) 19 IntellPropLBull 1.

Nicolas Zingales "The Brazilian approach to internet intermediary liability: blueprint for a global regime? " (2015) 4 IPR 4.

G Unpublished Texts

Emily B. Laidlaw "Internet Gatekeepers, Human Rights and Corporate Social Responsibilities" (Doctor of Philosophy thesis, London School of Economics and Political Science, 2012).

8 Press Releases

Peter Foster "What happened in Brussels?" *The Telegraph* (Online ed, London, 22 March 2016).

Samantha Whitle "Making a big deal of university students' needs" *Dominion-post* (Online ed, Auckland, April 9 2015).

Tommy Livingston "Police keeping an eye on Vic Deals Facebook group" *Dominion-post* (Online ed, Auckland, January 12 2016).

9 Conferences

Lilian Edwards "Role and responsibility of the internet intermediaries in the field of copyright and related rights." (Presented at conference in June 2011 before governmental and Industry Representatives, Commissioned by World Intellectual Property Organisation, Geneva , 2011).

10 Internet

Article19 "European Court strikes serious blow to free speech online" (2013) Article19 www.article19.org

Article19 "Internet intermediaries: Dilemma of Liability" (2013) Article19 <www.article19.org>

Facebook "How do I create a Page?" (2016) Facebook <https://www.facebook.com/help>

Joe McNamee "Guide to the Code of Conduct on Hate Speech" (3 June 2016) EDRi < https://edri.org/about/>.

Jyoti Panday "Comparative Study Of Intermediary Liability Regimes Chile, Canada, India, South Korea, UK and USA in support of the Manila Principles On Intermediary Liability" (1 July 2015) Manila Principles <www.manilaprinciples.org>.