Deep Pockets, Packets, and Harbors

THOMAS MARGONI & MARK PERRY*

Deep Packet Inspection is a set of methodologies used for the analysis of data flow over the Internet. It is the intention of this Paper to describe technical details of this issue and to show that by using Deep Packet Inspection technologies it is possible to understand the content of Transmission Control Protocol/Internet Protocol communications. These communications can carry publicly available content, private users' information, legitimate copyrighted works, and even infringing copyrighted works.

Legislation in many jurisdictions regarding Internet service providers' liability, or more generally the liability of communication intermediaries, usually contains "safe harbor" provisions. The World Intellectual Property Organization Copyright Treaty of 1996 has a short but significant provision excluding liability for suppliers of physical facilities. The provision is aimed at communication to the public and the facilitation of physical means. Its frequent application to cases of contributory or vicarious liability, in absence of specific national implementation, can prove problematic. Two of the most relevant legislative interventions in the field, the Digital Millennium Copyright Act and the European Directive on Electronic Commerce, regulate extensively the field of intermediary liability. This paper looks at the relationship between existing packet inspection technologies, especially the "deep version," and the international and national legal and regulatory interventions connected with intellectual property protection, and with the correlated liabilities exemptions. In analyzing these two main statutes, we will take a comparative look at similar interventions in Australia and Canada that can offer some interesting elements of reflection.[1]

TABLE OF CONTENTS

---

* Dr. Thomas Margoni is a Senior Researcher at the Instituut voor Informtierecht (IViR), Faculty of Law, University of Amsterdam, Netherlands. Professor Mark Perry is Professor of Law at the University of New England, Armidale, NSW, Australia, and also a Professor of Science and Professor of Law at the University of Western Ontario, Canada. The authors thank Sarah Nguyen (Western Law) for her hardworking research assistance and the IBM Center for Advanced Studies for its support. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7 2007–2013).

[1] These issues were discussed at the Ohio State Law Journal Symposium: The Second Wave of Global Privacy Protection (Nov. 16, 2012).

I. INTRODUCTION

The default requirement for Internet communications is that the data is sent to its destination as fast as possible. The Internet is based on Transmission Control Protocol/Internet Protocol (TCP/IP), which is used to achieve communications by chunking the data into "packets" that are sent over the network toward their destination. Individual packets making up the same communication may take different routes to get to their destination in the fastest, most efficient, and non-congested way. Packets of different kinds and sources travel together around the network. The priority for delivery is generally first-in-first-out, a design that implies that there is no packet discrimination based on the source, destination, content, type, carrier, etc. Every packet is treated equally. For example, every packet suffers the same latency, regardless of whether or not the packet is of a kind that is time-sensitive (e.g., audio–video packets are treated like e-mail packets, even though the effect of a delay in delivery is very different). It has been argued that the Internet has been so successful as a communication system largely due to this end-to-end design.[2]

From the Internet's conception, no prioritization of packets over its infrastructure was envisaged.[3] Some have argued that discrimination as to the handling of packets would increase network efficiency, and it is true that over a congested network it would be more efficient to prioritize those packets that are time sensitive.[4] For example, delay of voice-over Internet protocol packets may render the communication useless, but the same delay in the case of an e-mail would pass unnoticed. Network Neutrality advocates usually do not consider this technology-based efficiency as a threat.[5]

---

[2] *See* J.H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYS. 277 (1984); *see also* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930 (2001) (giving an overview of the architecture of end-to-end design, and its contribution to the growth of the Internet).

[3] For an early history of packet switching see, Lawrence G. Roberts, *The Evolution of Packet Switching*, 66 PROC. IEEE 1307, 1307 (1978); *see also* Lemley & Lessig, *supra* note 2, at 931, 944 (highlighting the nondiscriminatory nature of the end-to-end design and its early use in telephone cable lines).

[4] Jeane S.-C. Chen & Roch Guérin, *Performance Study of an Input Queueing Packet Switch with Two Priority Classes*, 39 IEEE TRANSACTIONS ON COMM. 117, 124 (1991).

[5] *See, e.g.*, Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 142 (2003); Thomas Margoni & Mark Perry, *Legal Consequences of Packet Inspection*, *in* PROCEEDINGS OF CYBERLAWS: THE SECOND INTERNATIONAL CONFERENCE ON TECHNICAL AND LEGAL ASPECTS OF THE E-SOCIETY 18, 19 (2011), *available at* http://ssrn.com/abstract=2028981.

II. THE TECHNOLOGY

To get a better understanding of the issues involved with Deep Packet Inspection (DPI), an overview of the protocols that are used to send information around the Internet and the nature and abilities of DPI is required.

A. *Transmission Control Protocol/Internet Protocol*

The Internet is made up of various layers of technology and protocols. For example, the physical structure requires that there is some channel for communication between devices, ranging from radio waves to fiber cables and boxes, known as routers, which direct the Internet traffic. Small and sub-$100 routers are becoming common in the networked home, but the cost can be very high for a core network router handling multi-Terabit per second throughput, such as those used by large Internet service providers (ISPs).

In *In re Doubleclick Inc. Privacy Litigation*,[6] a clear and simple description of the creation of the packets is given by the court:

> Packet switching works as follows. The computer wishing to send a document ("originating computer"), such as a music file or digital image, cuts the document up into many small "packets" of information. Each packet contains the Internet Protocol ("IP") address of the destination Web site, a small portion of data from the original document, and an indication of the data's place in the original document. The originating computer then sends all of the packets through its local network to an external "router." A router is a device that contains continuously-updated directories of Internet addresses called "routing tables." The router takes each packet from the original document and sends it to the next available router in the direction of the destination Web site. Because each router is connected to many other routers and because the connection between any two given routers may be congested with traffic at a given moment, packets from the same document are often sent to different routers. Each of these routers, in turn, repeats this process, forwarding each packet it receives to the next available router in the direction of the destination Web site. Collectively, this process is called "dynamic routing."[7]

Each device that uses the Internet requires an address. Internet Protocol version 4 (IPv4), which is still widely used, allowed for a little over four billion IP addresses.[8] These addresses are allocated by the Internet Assigned Numbers Authority (IANA), which is responsible for the global coordination of the Internet addressing system.[9] Although concern was expressed in the 1980s as to

---

[6] 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[7] *Id.* at 501.

[8] As IPv4 is a thirty-two bit address space, it has an absolute maximum address space of 2^{32} (i.e., two times two, thirty-two times, to equal 4,294,967,296).

[9] *IANA IPv4 Address Space Registry*, IANA, http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml (last updated May 20, 2013) ("Originally, all the

the limiting factor of the number of addresses, and working parties were set up to explore alternatives, it has only been over the last few years that the adoption of IP version 6 (IPv6)[10] has started to become more broadly adopted.[11] IPv6 allows for the addressing of 3.4×1038 (that is, 34 followed by 37 zeros) addresses.[12] IPv4 and IPv6 will coexist for some years to come. Regardless of which protocol is used, a text file or video sent over the Internet is broken into small chunks known as packets. These packets are reassembled at the destination to make up the original file that was sent. Each packet that goes across the Internet can be regarded as an "envelope" around the chunk of data that is being transmitted. This envelope consists of the required information to make sure that packets are not lost: the routing information is put into what is known as the "header" of the packet. When a router receives a packet it just has to look at the header of the packet to know where it is supposed to go, and the router forwards the packet to that destination. It is fundamental to TCP/IP that packets are managed in this way, and that they are reassembled when they have reached their destination. The information that is necessary for reassembly in the correct order is also contained in the packet header. Packets are received in random order, and may not follow the same physical route.[13] The structure of the headers for each packet is complex, and there is a lot more information contained in the header than simply the addressing of the packet; it will also include a lot more than just the sender and recipient addresses.[14]

It is clear that by looking at the header of a packet, a great deal of information can be gleaned as to the communications between the sender and the recipient, but the content of the packet, the information that makes up the

---

IPv4 address spaces [were] managed directly by the IANA. Later parts of the address space were allocated to various other registries to manage for particular purposes or regional areas of the world.").

[10] IANA announced the worldwide deployment of IPv6 fourteen years ago. *See Delegation of IPv6 Address Space*, IANA (July 14, 1999, 12:32 PM), http://www.iana.org/reports/1999/ ipv6-announcement.html.

[11] Cisco provides a global visualisation of IPv6 use on its website. *See IPv6 Deployment*, CISCO, http://6lab.cisco.com/stats/index.php (last visited July 10, 2013). In addition to greater address space in IPv6, there are many other differences from IPv4, including more efficient address header management.

[12] This is a very large number. In the United States, it would be 400 undecillions.

[13] INFO. SCIS. INST., UNIV. OF S. CAL., DOD STANDARD INTERNET PROTOCOL 7–9 (1980), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc760.txt.pdf.

[14] IPv6 includes at least the version, traffic class, flow label, length of the IPv6 payload, next header, and hop limit, which is a simplification of IPv4. *See* S. DEERING & R. HINDEN, NETWORK WORKING GRP., INTERNET PROTOCOL, VERSION 6 (IPV6): SPECIFICATION 4–5 (Dec. 1998), *available at* http://tools.ietf.org/html/rfc2460.

communication, is not revealed.[15] Routers have no need to examine such information. Routers need to determine what to do with a packet as fast as possible and to send it on its way.

B. *Deep Packet Inspection*

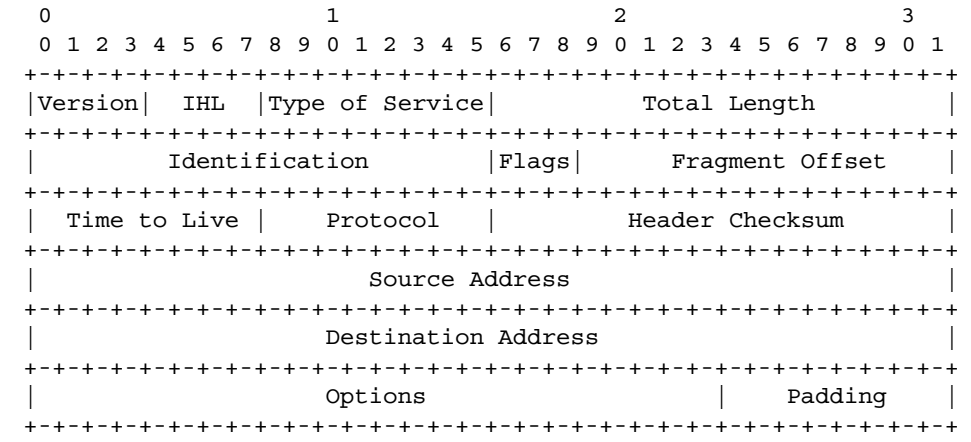
DPI includes a set of methodologies used for the analysis of data flow over the Internet. Clearly, for the Internet to function, the header information of packets must be read by routers. In contrast to this "shallow" packet inspection for functional purposes, DPI goes into the data content of the packet.[16] It is not the intention here to describe the full technical details of this issue, but rather show enough to demonstrate that by using DPI technologies, it is possible to understand more than the addressing details of TCP/IP communications.

The technologies used in DPI are, as with other information technologies, ever in development and advancement. In 2008, Deutsche Telekom made a submission to the European Commission's Consultation on "Creative Content Online in the Single Market" in which it stated:

> [With DPI, e]very IP frame must be decoded; many IP frames of a connection must be cached, consolidated and inspected to consider which type of protocol is used in an IP connection. The used protocol in the IP connection must be decoded, cached, consolidated and inspected as well, to find out, which type of data is transmitted in the connection. Since protocol tunnels are a common use,

---

[15] Look at a packet header:



INFO. SCIS. INST., UNIV. OF S. CAL., INTERNET PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL 11 (1981), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc791.txt.pdf.

[16] *See generally* Talitha Nabbali & Mark Perry, *Going for the Throat: Carnivore in an Echelon World—Part I*, 19 COMPUTER L. & SECURITY REV. 456 (2003); Talitha Nabbali & Mark Perry, *Going for the Throat: Carnivore in an ECHELON World—Part II*, 20 COMPUTER L. & SECURITY REV. 84 (2004) (both articles discussing these header tracing technologies and their use in government surveillance).

> it is possible, that the type of data is just another protocol, which must be decoded, cached, consolidated and inspected and so on.
> Once the used protocol is identified, a [sic] software is needed, which understands the protocol to interpret the transmitted data. If the connection itself or the transmitted data is encrypted with strong encryption methods, it is not possible to decrypt the transmitted data and to find out, which data or type of data is transmitted. Just using HTTPS [Hypertext Transfer Protocol Secure] (mostly known from home banking or web mail) makes it impossible for Deep Packet Inspection, to find out, which URL [uniform resource locator] is used (just the FQDN [fully qualified domain name] is known), which type of data is transmitted or which content was requested.[17]

The point Deutsche Telekom was making was that using DPI for the purpose of "such a general monitoring of the whole traffic of all of our customers regardless of whether a suspicion exists or not cannot realistically be an option for right holders to fight piracy."[18] However, the ability of the software available today allows for more information to be extracted, processed, and made available with less data. One DPI provider, for example, states that it developed DPX Network Probe for "lawful interception and network analysis in real-time,"[19] in cooperation with state authorities and law enforcement agencies. However, an amazing assertion was made just a year later from the same DPI vendor:

> It is a common claim that encryption and obfuscation prevent DPI systems from being able to classify the encrypted network flow. While it is true that plain pattern matching does not work with encrypted communication, modern DPI systems go beyond this simple method. They use behavioral and statistical analysis as described above. In fact, encryption has very little effect on the classification ability and accuracy of advanced DPI equipment.[20]

---

[17] DEUTSCHE TELEKOM, CONSULTATION ON "CREATIVE CONTENT ONLINE IN THE SINGLE MARKET" 15 (2008), *available at* http://ec.europa.eu/avpolicy/docs/other_actions/col_2008/comp/dtelecom_en.pdf.

[18] *Id.*

[19] *DPX Network Probe*, IPOQUE, http://www.ipoque.com/en/products/dpx-network-probe (last visited Sept. 14, 2013).

[20] KLAUS MOCHALSKI & HENDRIK SCHULZE, IPOQUE, DEEP PACKET INSPECTION: TECHNOLOGY, APPLICATIONS & NET NEUTRALITY 4–5 (2009), *available at* http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf (emphasis added). This quote must be seen in context; it is about P2P traffic:

> The common claim among P2P users and DPI opponents that the use of encryption and obfuscation in P2P networks like eDonkey and BitTorrent is a measure to ensure the users' privacy is plain dishonest. Even if encryption is enabled, files are still shared with the general public, so for everybody to download, store and read – of course in unencrypted format. This is also why encryption does not provide any protection against copyright investigations in P2P networks, where investigators use normal P2P clients to participate in the network and download files from potential infringers. The

The authors go on to reassure us that DPI does not enable "reading" of encrypted content and "DPI as such has no negative impact on online privacy."[21]

The vendors of DPI give much information on their abilities to read packets, and even if the packet data content is encrypted, it seems possible to "understand" the type of data involved in the communication. Indeed, using such techniques as DPI, it is possible to gain useful intelligence about the "network" that is being studied.[22] The privacy implications for Internet users by the adoption of DPI has been widely canvassed,[23] but here we are more interested in the relationship between the use of such technologies and the safe harbor sheltering offered by legislation for ISPs, discussed below. The issue of finding a deep pocket is one that should be on the mind of all litigators if the aim is to achieve compensation for damages.

III. DEEP POCKETS AND SAFE HARBORS

Litigation against those with deep pockets usually makes most sense when suing for copyright infringement and seeking to recover damages. In the United States, actions against infringers have led to very high judgments against individuals by relying on actual or statutory damages.[24] This is due to the desire

---

> only sensible reason for encryption is the attempt to circumvent bandwidth limitations imposed for P2P transfers by the ISP. However, with modern traffic management systems, which are able to reliably detect obfuscated and encrypted P2P traffic, this measure is totally ineffective.

Id. at 5.

[21] *Id.* at 7.

[22] GRAHAM FINNIE, QOSMOS & HEAVY READING, THE ROLE OF DPI IN AN SDN WORLD 13 (2012), *available at* http://www.qosmos.com/wp-content/uploads/2013/03/Heavy_Reading-Qosmos_DPI-SDN-WP_Dec-2012.pdf. Heavy Reading reports that in 2011, investment in DPI exceeded half a billion dollars. *Id.* at 9.

[23] *E.g.*, Christopher Witteman, *Information Freedom, a Constitutional Value for the 21st Century*, 36 HASTINGS INT'L & COMP. L. REV. 145, 187 n.141 (2013) (although Witteman makes little of the issue); *The Privacy Implications of Deep Packet Inspection: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. on Commc'ns, Tech. & the Internet*, 111th Cong. 1–2 (Apr. 23, 2009) (statement of Leslie Harris, Pres. and CEO, Center for Democracy & Technology), *available at* https://www.cdt.org/files/pdfs/20090423_dpi_testimony.pdf.

[24] Actual damages allow the plaintiff to recover the copyright owner's actual damages and any additional profits of the infringer. Statutory damages are in the range of $750 to $30,000 at the discretion of the court. Statutory damages can be lowered to $200 in the case of innocent infringement or raised to $150,000 in case of willful infringement. 17 U.S.C. § 504(c)(1)–(2) (2012). Punitive damages have traditionally been excluded for cases of copyright infringement, since the punitive purpose is generally achieved through the reported increase in case of willful infringement. *See, e.g.*, On Davis v. GAP, Inc., 246 F.3d 152, 172 (2d Cir. 2001); Oboler v. Goldin, 714 F.2d 211, 213 (2d Cir. 1983).

to make examples of infringers and to punish them.[25] However, even in the United States, these actions have not won general approval from the public at large.[26] An alternative target would be to sue the ISP, whether the gateway host or content host. Intermediaries such as service, hosting, and content providers are usually public companies or large corporations, which means that they are much more solvent. Further, being that their activities and information are public, they can be easily identified, and suing a few big and solvent companies is easier than going after a myriad of individual users. However, one of the issues that a potential litigant needs to face is the shelter that is provided for ISPs in many jurisdictions, known as safe harbor legislation.

The World Intellectual Property Organisation Copyright Treaty (WCT) may be seen as the root for consensus on providing exclusion of liability to providers of physical facilities for Internet communications, i.e., for ISPs. This comes from the Agreed Statements on Article 8 of the WCT providing:

> It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11bis(2).[27]

Article 8 of the WCT creates a general right of communication to the public—a novel approach at the time in copyright at the international level[28]—and the scope of the Agreed Statements is to clarify that the mere provision of physical facilities for enabling a communication is not tantamount to an act of communication itself, which otherwise would be infringing the newly created right. Although not a detailed basis for regulation of the field, the Agreed Statements on Article 8 can certainly be seen as an important principle placed in one of the major international instruments in the field of copyright law. This was particularly important during a time when the role played by intermediaries

---

[25] *See, e.g.*, Sony BMG Music Entm't v. Tenenbaum, 660 F.3d 487, 489–90 (1st Cir. 2011) (Sony received $675,000 in damages after a judgment was entered against defendant Tenenbaum for copyright infringements of thirty songs when he was a twenty-year-old student.).

[26] Kristina Groennings, *Costs and Benefits of the Recording Industry's Litigation Against Individuals*, 20 BERKELEY TECH. L.J. 571, 589 (2005); *see also* Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 CARDOZO ARTS & ENT. L.J. 725, 729–30 (2005).

[27] *Agreed Statements Concerning the WIPO Copyright Treaty*, WORLD INTELL. PROP. ORG. (Dec. 20, 1996) [hereinafter *Agreed Statements WIPO*], http://www.wipo.int/treaties/en/ip/wct/statements.html.

[28] Prior to this, the right to communication to the public was contained in different provisions dealing with specific subject matter or type of authors. *See* Berne Convention for the Protection of Literary and Artistic Works arts. 11(1)(ii), 11bis(1)(i)–(ii), 11ter(1)(ii), 14(1)(ii), 14bis(1), Sept. 9, 1886, revised at Stockholm, July 14, 1967, 828 U.N.T.S. 221.

in online communication was far from clear in the limited but growing case law available.[29]

Article 8 and the connected Agreed Statements express the rule that the mere provision of physical facilities that enable a communication to the public does not constitute an act of communication to the public by itself, and therefore excludes liability for direct copyright infringement. However, under the general law of torts (differences among legal systems, especially between common law and civil law traditions, will not be addressed in this Paper), liability can be found not only for acts of direct infringement, but also where a subject facilitates or has a causational role in the line of events conducive to the tortious event.[30]

By virtue of the Agreed Statements of Article 8, ISPs can be considered exempted from direct liability when their actions are limited to the provision of the physical means necessary for an online communication.[31] However, they can still be found liable for acts of indirect infringement, at least as long as the right of communication to the public of copyrighted material is involved, and as long as we assume that ISPs provide physical facilities and not software ones.[32] Interestingly, the World Intellectual Property Organization (WIPO) Performances and Phonograms Treaty, signed simultaneously with the WCT, lacks any such limitation of liability.[33]

---

[29] During the 1990s, courts had occasion to decide on the issue of online intermediaries' liability, especially in the United States, but followed different uncoordinated approaches. *See, e.g.*, Playboy Enters. v. Frena, 839 F. Supp. 1552, 1556–59 (M.D. Fla. 1993) (finding a Bulletin Board Service liable for copyright infringement even though it did not upload the work nor had knowledge of the infringing activity); *see also* Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of the Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 348–49, 353–55 (1995) (discussing several circuit court approaches to liability in this context); KAMIEL KOELMAN & BERNT HUGENHOLTZ, INST. FOR INFO. LAW, UNIV. OF AMSTERDAM & WORLD INTELLECTUAL PROP. ORG., WORKSHOP ON SERVICE PROVIDER LIABILITY: ONLINE SERVICE PROVIDER LIABILITY FOR COPYRIGHT INFRINGEMENT 12 (1999), *available at* http://www.ivir.nl/publicaties/hugenholtz/wipo99.pdf (discussing a shift among courts from rigid imposition of copyright liability on online intermediaries to more relaxed approaches). For a case of exclusion of liability, see the landmark case Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361, 1373 (N.D. Cal. 1995); *see also* Jerome H. Reichman et al., *A Reverse Notice and Takedown Regime To Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 983 (2007) (highlighting the competing interests to be addressed in safe harbor legislation, including copyright liability for ISPs).

[30] As, for instance, clarified by the court in *Netcom*, 907 F. Supp. at 1373.

[31] *See Agreed Statements WIPO*, *supra* note 27 (The Statements clarify the meaning of the Berne Convention for the Protection of Literary and Artistic Works as it relates to digital versions of such works.).

[32] *See id.*

[33] *See generally* WIPO Performances and Phonograms Treaty (WPPT), Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), *available at* http://www.wipo.int/edocs/lexdocs/treaties/en/wppt/trt_wppt_001en.pdf.

An exemption of liability limited to the provision of physical facilities becomes quite unrealistic today when we have vast social networks and widespread adoption of Web2.0, i.e., where the provision of services and software is the key technological and economic activity. However, in 1996, the provision in the WCT represented an acceptable compromise at the international level.

The two main pieces of legislation that have regulated in a detailed manner the ambit of ISPs' liability at the national level are the Digital Millennium Copyright Act (DMCA)[34] and (indirectly) the Electronic Commerce Directive (ECD).[35] The DMCA updated the Copyright Act of 1978 by introducing into U.S. law those provisions that create specific zones of (secondary) liability exemptions for qualifying ISPs when meeting certain conditions.[36]

The ECD has done something quite similar for the European Union (EU).[37] Note that under EU law, a Directive represents a piece of "framework" legislation, directed to Member States of the EU, which have the obligation to implement it into their domestic legal systems within the provided time limits. During the process of implementation, Member States are usually left with (explicit or implicit) margins of operations, thereby rendering every national implementation potentially different but "harmonized." When we analyze the liability exemptions set forth by the ECD, we are looking at a system that is the reference for the whole EU. That being said, specific implementation in each Member State is sometimes the key to understanding how liability exemptions work in EU countries, since national courts have proven to be quite attached to their traditional construction of tortious liability.[38]

Another major difference between the DMCA and the ECD resides in the different ambits of application. In fact, the DMCA, as we have seen, amends the Copyright Act[39] and applies to copyright infringements. If liability limitations exist outside the realm of copyright law in the United States, it is by virtue of specific acts that regulate specific ambits (for example, Section 230 of the

---

[34] Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860.

[35] Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC) [hereinafter Electronic Commerce Directive].

[36] *See generally* Digital Millenium Copyright Act (categories of service providers and various factors in determining exemption throughout the Act).

[37] Although an EU Directive is not directly applicable to Member States, its scope is to establish a harmonized legal framework within which EU Member States enact specific national rules to comply with the Directive.

[38] *See, e.g.*, Tribunale di Milano [Tribunal of Milan], Reti Televisive Italiane S.p.A. (RTI) c. Italia On Line s.r.l. (IOL) 20 gennaio 2011, n. 7680/2011; Cour d' appel [CA] [regional court of appeal] Paris, Google Inc. v. Bac Films, Jan. 14, 2011 (partially confirmed, partially remanded by Cour de cassation Arrêt n° 828 du juillet 2012).

[39] *See* Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541; A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965 (2013).

Communications Decency Act (CDA) of 1996),[40] or because the system set up by the DMCA has been used as a sort of reference model by U.S courts (as it has been observed sometimes in the case of trademark law).[41]

The ECD, on the contrary, applies horizontally to any illegal information or activity happening on a service of the information society (the Internet for our purposes). Therefore, the system of indirect liability exemptions set forth by the ECD will be relevant for cases of alleged copyright infringement, as well as for cases of defamation, or limitations of the right to freedom of expression, privacy violations, or any other act that can be considered illegal.

Entering more into the specific details of the two statutes, we can observe a similar approach in the regulation of ISP liability. Both identify different types of intermediaries operating as service providers, and set forth conditions and obligations that need to be fulfilled in order for those intermediaries to be exempted, at least from monetary liabilities.[42] Under specific circumstances, ISPs can be the target of injunctions from courts or even administrative bodies aimed at the removal of the identified illegal content or copyright infringing material.[43]

Access providers offer Internet access to their subscribers, who use the cables, wires, routers, and connectivity in order to access the Internet, connect to websites, upload and download information, and any other online activity one can think of. It is clear that, from a causation point of view, this type of ISP represents an essential element of the existence of the "network," and thus can be found indirectly liable in a case of copyright infringement, since without its intervention the tortfeasor (e.g., the user illegally uploading a song) would not have been able to perpetrate his or her infringing activities. To be exempted from contributory liability, this type of intermediary needs to operate as a mere conduit.[44] It needs to refrain from activities such as initiating the transmission, selecting the content, selecting the recipient, modifying the content, or making copies of the content, in addition to those activities for intermediate or transient storage, which in any case cannot be made accessible to anybody other than the

---

[40] Telecommunications Act of 1996, Pub. L. No. 104-104, § 501, 110 Stat. 133 (The Telecommunications Decency Act is the popular name for Title V of the Telecommunications Act.).

[41] Trademarks, for example, are not covered by Section 230 of the CDA, nor by the DMCA. Therefore a website hosting an infringing trademark uploaded by one of its users could be found liable upon reception of a notice to take it down. Even if such notice is not proper of the trademark world, there will be a strong incentive for the website to take such content down. Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 104–05 (2007).

[42] *See* 17 U.S.C. § 512(a)–(c) (2012); Electronic Commerce Directive, *supra* note 35, arts. 12–14.

[43] 17 U.S.C. § 512(a)–(c); Electronic Commerce Directive, *supra* note 35, arts. 12(3), 13(2), 14(3).

[44] *See* 17 U.S.C. § 512(a); Electronic Commerce Directive, *supra* note 35, art. 12.

intended recipient and cannot be accessed beyond the period of time necessary for the transmission.[45]

A second type of intermediary identified by both statutes is that of a caching provider.[46] This intermediary creates copies of the content made available by users to enhance the efficiency of the network (a common practice on the Internet that occurs without users noticing).[47] In the case of caching, the intermediary is not liable with regard to those copies as long as it does not modify the information copied, it complies with rules regarding access, updating, and refreshing, it does not interfere with the lawful use of technology widely recognized and used by industry to obtain data on the use of the information, and it

> acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[48]

A third type of intermediary identified by both the EU and the United States regards hosting providers.[49] A service provider that offers storage services at the direction of users is not subject to liability, as long as the provider is ignorant of the presence of such infringing content, does not receive direct financial benefit attributable to the infringing material (conditions present only in the DMCA), and acts expeditiously to remove such content upon acquiring such knowledge.[50] The absence of the requirement of no financial benefit is not the only major difference between the DMCA and the ECD. In fact, the way in which such knowledge of content can be acquired is extensively regulated in the DMCA, while it is almost completely absent in the ECD. The latter only mentions a general possibility for Member States to implement procedures governing the removal of such information.[51]

---

[45] *See* 17 U.S.C. § 512(a); Electronic Commerce Directive, *supra* note 35, art. 12(1). The specific wording of these two provisions is in fact quite similar.

[46] 17 U.S.C. § 512(b); Electronic Commerce Directive, *supra* note 35, art. 13.

[47] Caching is a very common practice on the Internet. In order to reduce the distance that a transmission has to cover for every single connection, local copies in intermediate positions on the network are created so that connections can easily reach such closer copies instead of travelling all the way to the source. *See* Electronic Commerce Directive, *supra* note 35, art. 13(1) (describing the process of caching).

[48] *Id.* art. 13(1)(e). See 17 U.S.C. § 512(b)(2)(E) for a rule with a similar effect, although the wording of this provision is much more detailed than that of the Directive.

[49] Electronic Commerce Directive, *supra* note 35, art. 14; 17 U.S.C. § 512(c).

[50] Electronic Commerce Directive, *supra* note 35, art. 14; 17 U.S.C. § 512(c).

[51] Electronic Commerce Directive, *supra* note 35, art. 14(3) ("This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an

This difference in approach is at the core of the current transatlantic debate regarding ISP liability. We have seen how similar the relevant provisions are in creating areas of secondary liability exemptions, also known as safe harbors. The three types of intermediaries analyzed are similarly defined, and the conditions that they have to meet to enjoy such exemptions are comparable. It is true that the DMCA (as well as the Canadian Copyright Modernisation Act of 2012[52]) identifies a fourth category of intermediaries that the ECD does not, i.e., Information Location Tools (search engines).[53] For the purpose of the present analysis this is an aspect that can be put aside.[54] The aspect that has driven much of the current debate, especially at the EU level, is the necessity for a system of notice and take-down, similar to that of the United States. Indeed, twelve years after the implementation of the ECD, the creation of procedures for the notification and removal of illegal information has not emerged with the promptness and coherency that the EU legislature probably had in mind when drafting the already mentioned Article 15(2) of the ECD, for example, as witnessed by Recital 40.[55] Member States have failed to implement generalized procedures to remove content upon receipt of specific notifications, and courts have found themselves in the place that the EU legislature had originally reserved for national parliaments and governments: deciding the content and effects of those notices that right-holders have started to address also to non-U.S.-based providers.

A brief summary regarding the DMCA requirements for a notice and take-down procedure is at this point beneficial. As we have seen, absence of actual knowledge is a key factor to ISPs' enjoying the safe harbor provision for

---

infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.").

[52] *See* An Act To Amend the Copyright Act, S.C. 2012, c. 20 (Can.).

[53] *See* 17 U.S.C. § 512(d); Copyright Act, R.S.C. 1985, c. C-42, art. 41.27 (Can.).

[54] In a case involving Google and its search engine activity, the European Court of Justice found that Google operated as a hosting provider. *See* Case C-236/08, Google France S.A.R.L. v. Louis Vuitton Malletier SA, 2010 E.C.R. I-2467, I-2510–11.

[55] *See* Electronic Commerce Directive, *supra* note 35, at 6 ("Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.").

copyright infringement caused by users of storage services.[56] Such knowledge can be acquired upon receipt of a specific notice sent by right-holders.[57] The service provider has to implement specific measures if it wants to qualify under the safe harbor provisions.[58] First, it has to designate an agent to receive notifications of claimed infringement.[59] It has to make the relevant information regarding the notification system for potential infringements available on its website in a location accessible to the public. The agent is the person who receives notices that must be written and signed, and that contain information on the work allegedly infringed, the infringing material, and the complaining party.[60] The complaining party must have a good faith belief that the complaints and the information provided are accurate.[61] A notice that does not contain all the information required by the Act cannot be considered appropriate to trigger the threshold knowledge required by providers for a finding of liable conduct.[62] Once the notice in proper form has been received by the agent, the content has to be taken down or access to it disabled.[63] The provider will in no circumstance be held liable for the removal (including content that eventually proves to be non-infringing) as long as the notification sent follows the above-mentioned rules and as long as the provider takes reasonable steps to promptly notify the subscriber of the removal. The subscriber, in turn, can counter-notify the ISP through the same agent, claiming that he has a good faith belief that the removed material was not infringing.

The counter-notice requirements are similar to those of the notice. Such counter-notification has to be forwarded to the original notification issuer with the warning that within ten business days the material will be restored, and restore it in ten to fourteen days, unless the agent receives a notification informing him or her that an action has been filed for a court order to stop the infringing activity.[64] This represents a succinct summary of the main provisions contained in the DMCA regarding the take-down procedures following the receipt of a proper notice. The detail with which the legislature has framed the DMCA provision stands out when compared to the EU equivalent.

If we turn our attention to the EU ECD and its "equivalent" provision, we immediately see how scarce are the directions given with regard to the removal of illegal content procedures. Such an approach is opposite to that employed by the DMCA, by an act that otherwise has followed closely its U.S. counterpart. Comparison with the Canadian and Australian legislation shows further differences.

---

[56] *See* 17 U.S.C. § 512(c)(1).
[57] *See id.*
[58] *Id.* § 512(c)(1)–(2).
[59] *See id.*
[60] *Id.* § 512(c)(2)–(3).
[61] *See id.* § 512(c)(3).
[62] 17 U.S.C. § 512(c)(3).
[63] *Id.* § 512(c)(1).
[64] *Id.* § 512(g)(2)(C).

The Canadian approach with regard to the notification procedures is interesting in this specific regard. Notably, the sections regarding the notice and notice provision (41.25 and 41.26) are approved but not yet in force. On the one hand, it follows a structure similar to the DMCA in the details that notifications should possess, but with a major difference concerning the obligations of the receiver of such a notification. The intermediary that receives a proper notice does not have an obligation to remove or disable access to the allegedly infringing content.[65] Its only obligation is to forward such notice to the user that has uploaded such content.[66] As long as the intermediary operates as a communication forwarder between the copyright-holder and the user, it is exempted from liability.[67] Such a system takes the name of "notice-and-notice."[68] The legislative summary of Bill C-11 (An Act To Amend the Copyright Act), states that "concern has been raised that a 'notice-and-takedown' regime could create incentives for ISPs to remove content without warning or evidence of actual infringement, which can potentially lead to a stifling of free expression" and "the Privacy Commissioner of Canada raised concerns about the privacy implications of requiring ISPs to retain personal information for the purposes of the regime."[69]

As previously pointed out, it is too early to say how this novel approach to balancing the interests of the stakeholders will pan out.

Australia has broad safe harbor provisions, while employing yet another approach. Division 2AA of Part V of the Australian Copyright Act provides

---

[65] *See* An Act To Amend the Copyright Act, S.C. 2012, c. 20, art. 41.27 (Can.).

[66] *Id.*

[67] *Id.*

[68] Copyright Act, R.S.C. 1985 c. C-42, arts. 41.25, 41.26, 41.27(3) (Can.) (brought in by An Act To Amend the Copyright Act, S.C. 2012, c. 20 (Can.)). These will come into effect only following a consultation process and Order-in-Council.

> 41.26 (1) A person described in paragraph 41.25(1)(a) or (b) who receives a notice of claimed infringement that complies with subsection 41.25(2) shall, on being paid any fee that the person has lawfully charged for doing so,
> (a) as soon as feasible forward the notice electronically to the person to whom the electronic location identified by the location data specified in the notice belongs and inform the claimant of its forwarding or, if applicable, of the reason why it was not possible to forward it; and
> (b) retain records that will allow the identity of the person to whom the electronic location belongs to be determined, and do so for six months beginning on the day on which the notice of claimed infringement is received or, if the claimant commences proceedings relating to the claimed infringement and so notifies the person before the end of those six months, for one year after the day on which the person receives the notice of claimed infringement.

Id. art. 41.26.

[69] See Dara Lithwick & Maxime-Olivier Thibodeau, Parliament of Canada, Legislative Summary of Bill C-11 § 3.2.3 (rev. 2012), *available at* www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=c11&parl=41&Ses=1.

protection for "Carriage Service Providers" that limits the liability of ISPs in actions against them "for infringements of copyright that relate to the carrying out of certain online activities."[70] If an ISP is "providing facilities or services for transmitting, routing or providing connections for copyright material, or the intermediate and transient storage of copyright material"[71] whilst executing those services, relief is limited to terminating a specific account or to taking "reasonable steps to disable access to an online location outside Australia."[72]

In *Roadshow Films Pty Ltd. v iiNet Ltd.*,[73] the High Court of Australia found that the conduct of iiNet did not constitute "authorisation of its customers' copyright infringement" even though they had knowledge of the infringements. There was no obligation for iiNet to take action against such infringers.

EU ECD Article 14(3) reads, "This Article shall not affect the possibility . . . for Member States of establishing procedures governing the removal or disabling of access to information."[74] Such a provision leaves up to Member States the decision of whether and how to implement a system of notice and take-down.[75]

So far, no country has set up a detailed system of notice and take-down at the legislative level. France stands out, since it actually created a system of notice and take-down in its Confidence in the Digital Economy Act.[76] While such a procedure contained in Article 6.I.5 of the Act is only optional, it is one way to activate the knowledge requirement of the intermediary. Interestingly, however, courts have consistently interpreted such provision as being the liability-trigger requirement for ISPs, turning the legislative optional way into a de facto mandatory procedure.[77] This is in spite of the French Constitutional Council provision, that there is no obligation to remove a notified illegal content unless it is manifestly illegal, expressed in a 2004 decision.[78] Other countries have attempted to regulate the field of notification procedures, but without much success. This is due to institutional and general public acceptance issues, for example, in the case of Italy. The Italian Telecommunications Authority—*Autorità per le Garanzie nelle Comunicazioni* (AGCOM)—has taken different

---

[70] Copyright Act 1968 (Cth) s 116AA(1) (Austl.).

[71] *Id.* s 116AC.

[72] *Id.* s 116AG.

[73] (2012) 286 ALR 466, 466 (Austl.).

[74] Electronic Commerce Directive, *supra* note 35, at 13.

[75] *See, e.g.*, *id.* at 6.

[76] *See* Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [Law 2004-575 of June 21, 2004 on Confidence in the Digital Economy], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 22, 2004, at 11168.

[77] *See generally* Catherine Jasserand, *Critical Views on the French Approach to "Net Neutrality,"* J. INTERNET L. 18 (2013) (discussing the net neutrality debate in France spurred by the adoption and implementation of the revised European telecom rules).

[78] *See* Conseil constitutionnel [CC] [Constitutional Court] decision No. 2004-496DC, June 10, 2004, J.O. 11182 (Fr.).

steps towards the creation of a notice and take-down procedure, but has not been able to bring these steps to conclusion yet.[79] Currently, a proposal of regulation has been issued and is open for public comment.[80] The proposal sets forth a system of notice and take-down and creates an administrative body (a section of the AGCOM) that will have the power to order the removal of infringing content, or disablement of access in case of foreign websites, when the notified intermediary does not proceed to the removal by itself. The proposal seems to still be in an early stage, and many concepts (such as the difference between access, caching, and hosting providers) are not defined. The proposed regulation seems to need some refining before an objective analysis can be developed.

The fact that EU Member States have failed or demonstrated scarce interest in the regulation of notification procedures for the removal of illegal content should not suggest that the issue of notice and take-down has disappeared from the EU agenda or from the courts' case law.

In January 2012, the European Commission (EC) announced an initiative on "notice-and-action" procedures in their Communication on e-Commerce and other online services.[81] In such Communication, the EC calls for a "horizontal European framework for notice and action procedures"[82] and for a system "to combat illegal content more effectively and in a manner which upholds the internal market and fundamental rights by improving the framework for civil law proceedings."[83] In the wording of the EC, "'Notice-and-action' procedures begin when someone notifies a hosting service provider . . . about illegal content on the internet. . . . [They] are concluded when a hosting service provider acts against the alleged illegal content."[84] As a result of a 2010 public consultation on e-Commerce,[85] stakeholders indicated that these procedures "should lead to a quicker takedown of illegal content, should better respect

---

[79] *See* Press Release Autorità per le Garanzie nelle Comunicazioni (AGCOM), Draft Regulations on On-Line Copyright Protection Approved (July 25, 2013), *available at* http://www.agcom.it/default.aspx?DocID=11592.

[80] *See* Delibera N. 452/13/CONS, Consultazione pubblica sullo schema di regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo, AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM) (Apr. 9, 2003) (It.).

[81] *Commission Communication for a Coherent Framework for Building Trust in the Digital Single Market for E-Commerce and Online Services*, at 15, COM (2011) 942 final (Nov. 1, 2012) [hereinafter *Commission Communication*].

[82] *Id.* at 13.

[83] *Id.* at 14.

[84] *See Notice-and-Action Procedures*, EUROPEAN COMMISSION, http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm (last visited Sept. 10, 2013).

[85] *Public Consultation on the Future of Electronic Commerce in the Internal Market and the Implementation of the Directive on Electronic Commerce (2000/31/EC)*, EUROPEAN COMMISSION, http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm (last visited Sept. 10, 2013).

fundamental rights (in particular the freedom of expression) and should increase legal certainty for online intermediaries."[86] Furthermore, in June 2012, the EC launched a public consultation on procedures for dealing with illegal content on the Internet, titled: *A Clean and Open Internet*.[87] The consultation involves the issue of notification of illegal content, exploring issues such as whether service providers should put in place mechanisms to notify illegal content that are easy to find and easy to use, and if so, whether illegal content should exclusively be notified by such mechanisms or whether other alternative routes should be followed. The consultation also concerns acting on illegal content and explores issues related to service providers' roles in consulting the uploaders of alleged illegal content and whether they should provide feedback to notice providers.[88]

In light of the aforementioned, the direction of the EC's agenda in the field of ISP liability seems clear, i.e., a horizontal system of notification and action that includes the removal of illegal material, similar to the one adopted a decade ago by the U.S. legislature, but applied generally to all online illegal information and activities. Such an approach would certainly have the advantage over its North American counterpart to offer a unique scheme for safe harbor, instead of a system where copyright follows one route, patent and trademark a different one, and defamation, yet another one.

After all, a system of notice-and-action (a term that includes, but is not limited to, a take-down) is already partially implemented in the EU, as witnessed by industry and commercial practice and recognized to some extent also by courts.[89] In particular, the European Court of Justice has delivered a few decisions that have clarified interpretations connected with the removal of illegal information from the Internet.

In the landmark case *L'Oréal SA v. eBay International AG*, the European Court of Justice clarified that a notice for the removal of allegedly infringing content "cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated."[90] Therefore, under current EU law, a notification does not represent a tool that automatically triggers the requirement of actual knowledge on the recipient and thus exempts the recipient from the safe harbor.

---

[86] *Notice-and-Action Procedures*, *supra* note 84.

[87] *A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries*, EUROPEAN COMMISSION, http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm (last updated Apr. 9, 2012).

[88] *See id.*

[89] See Memorandum of Understanding, European Commission (May 4, 2011), *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf, for an example of industry position, signed in Brussels by representatives of the sector.

[90] Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-6011 ¶ 122.

The court added that in specific cases, such notification can indeed achieve the goal of triggering liability,

> [for] such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.[91]

If the EU decides to go in the direction chosen more than a decade ago by the DMCA, it might want to keep in mind what a decade ago was probably unforeseen, i.e., the number of notifications received by big ISPs. The few of them that have a transparency policy report as the most recent figures around four million notifications per week.[92] The reliance on the private sector ability to protect fundamental rights, in light of the costs that a careful procedure of analysis of notification requires, is an aspect that needs a profound assessment.

Another central aspect of ISP liability involves a general monitoring obligation on ISPs. Under EU law, general monitoring obligations are generally prohibited, as clearly established by Article 15 of the ECD: "Member States shall not impose a general 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."[93] General monitoring obligations have been defined as requiring "active observation of all electronic communications conducted on the network of [an intermediary] and, consequently, would encompass all information to be transmitted and all customers using that network."[94] This is usually done by employing extremely intrusive technologies such as DPI. As seen in the first part of this Paper, such tools—in order to identify the illegal content—have the ability to access all parts of all the packets (the smallest units of information transmitted on the Internet) that are sent during an online communication.[95]

This would allow intermediaries to actually intercept and read everything sent over a specific network. As in many other fields of law, the protection of some rights (those threatened by illegal content such as defamatory publications, counterfeited wares, privacy violations, etc.) can cause harm to other rights (those of the parties that conduct legitimate activities: Internet subscribers' freedom of expression and protection of personal data, intermediaries' freedom of economic initiative, right-holders' IP rights, etc.).

---

[91] *Id.*

[92] *See, e.g.*, *Transparency Report: Requests To Remove Content*, GOOGLE, http://www.google.com/transparencyreport/removals/copyright (last visited Sept. 10, 2013).

[93] *See* Electronic Commerce Directive, *supra* note 35, at 13.

[94] Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs S.C.R.L. (SABAM), http://curia.europa.eu ¶ 39 (Nov. 24, 2011).

[95] *See* Margoni & Perry, *supra* note 5, at 20.

The fundamental rights contained in the Charter of Fundamental Rights of the EU (EU Charter), together with the human rights contained in the European Convention of Human Rights (ECHR), are all of equal weight, and none is deemed superior to any other.[96]

In *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, the European Court of Justice made clear that the protection of the fundamental right to property, which includes the rights conferred by intellectual property, must be balanced against the protection of other fundamental rights.[97] Among such rights, specific attention has been paid to individuals' rights to protection of personal data and their freedom to receive or impart information, and ISPs' rights to conduct business (rights safeguarded by Articles 8, 11, and 16 of the EU Charter, respectively).[98] The European Court of Justice has called for "an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order," an interpretation which would further respect other fundamental rights and "the other general principles of Community law, such as the principle of proportionality."[99] The principle of proportionality in particular is a fundamental principle that permeates the EU legal order. It is recognized at the highest level at Article 5 of the Treaty on the EU, and it has been repeatedly analyzed (even outside the specific area of law we are proposing to study here) by European Court of Justice case law and the literature.[100]

The DMCA has no clear provision prohibiting general monitoring obligations.[101] However, in a 2010 decision, a United States district court found that under the DMCA, no general obligations to filter content exist for the intermediary, and the obligation to identify infringing content lies on the right-holder.[102] This decision was overturned in part and remanded to the district

---

[96] *See Scarlet*, Case C-70/10 ¶ 43.

[97] Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-271 ¶ 65.

[98] *Id.* ¶¶ 46–50.

[99] *Id.* ¶ 68.

[100] *See* Case C-331/88, The Queen v. Minister of Agri., Fisheries & Food, 1990 E.C.R. I-4057, I-4062; C-210/00, Käserei Champignon Hofmeister v. Hauptzollamt Hamburg-Jonas, 2002 E.C.R. I-6482, I-6492; *see also* XAVIER GROUSSOT, GENERAL PRINCIPLES OF COMMUNITY LAW 145–60 (2006); Jan H. Jans, *Proportionality Revisited*, 27 LEGAL ISSUES ECON. INTEGRATION 239, 239 (2000).

[101] *See* 17 U.S.C. § 512(m) (2012):

> Protection of Privacy.— Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—
>
> (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or
>
> (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

court, which ruled consistently with its first decision.[103] The case is currently on appeal.

IV. CONCLUSION

The limitations on the liability of ISPs possess common traits across the countries herein surveyed. Such similarities can be traced back to the general principle set forth in the Agreed Statements on Article 8 of WCT regarding acts of direct infringement of the right of communication to the public, and—on a much more detailed level—to national (and EU) legislative interventions. The DMCA and the ECD represent the most advanced examples of such legislation, with countries such as Canada and Australia following a similar direction, although through different approaches. Canada in particular might represent an interesting approach by offering a different balance to the interests involved, one that allegedly offers higher protection for freedom to communicate and users' rights over acts of alleged copyright infringement. The future application of such a provision should be followed with close attention.

It must be borne in mind that the choice of where to allocate liability for users' infringements is a public policy choice. To burden ISPs with a duty to actively control every aspect of information flow across their part of the network and to monitor every server might very well support the interests of the right-holders. However, such a scheme would hardly lower the number of infringements, and would only provide a much more solvent co-tortfeasor that right-holders can target with their damage claims. If, by using sophisticated monitoring, the service providers gain knowledge of the infringing content, then they become a suitable target—they have relatively deep pockets and are easy to identify. Furthermore, legal actions for tens of millions of dollars brought against a public company are much better accepted by society and the market than those brought against individuals.

However, to allocate such responsibility completely to ISPs— beyond the compromise currently in place—would create an obstacle to ISPs' operations, and likely deter investment in the Internet infrastructure and the evolving network ecosystem. It must be pointed out that Internet related activities account for 21% of GDP growth and for 25% of job creation in at least the G8 economies.[104] Indeed, from this point of view, to allocate liability to ISPs could be seen as holding shareholders of limited liability companies liable for the company debts beyond the face value of their shares. The legal limitation of investors' liability to their company's debts matured, not accidentally, during

---

[102] *See* Viacom Int'l v. YouTube, 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010).

[103] *See* Viacom Int'l v. YouTube, No. 07 Civ. 2103 (LLS), 2013 WL 1689071, at *5, *11 (S.D.N.Y. Apr. 18, 2013).

[104] *See Commission Communication*, *supra* note 81, at 1; *see also* MATTHIEU PÉLISSIÉ DU RAUSAS ET AL., INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS, AND PROSPERITY (2011).

the Industrial Revolution. If investors were to be considered liable beyond the face value of their shares, they probably would not embark on the most dangerous and risky enterprises—those that lead to the creation of innovative industries, new trade routes, and novel products.

From a policy perspective, development and innovation were favored over those business models that had reached maturity. It was a choice based on efficiency principles. Its intrinsic fairness can be disputed. From the perspective of creditors who see their credit paid only up to a small percentage, if at all, when the companies fail it is clearly an unfair solution, since they are held liable for the risk-taking activities (but not of the related revenues) undertaken by the company. Nonetheless, nation states have decided to allocate risks and costs in this specific way to favor and incentivize innovation and investment over rent-seekers, because at the end of the day, the global welfare would be greater for the entire society (although distributed quite differently from the previous status quo). The very same reasoning can be applied to ISPs' liability. To burden them with liability for users' acts would stifle Internet-based innovation and frustrate further investment in such market sector.

There is a second strong argument against the allocation of more liability to ISPs. This second argument is based not on a law and economic perspective, but on a fundamental rights one. As we have seen in our study, the technologies that ISPs already use, and would employ to a much greater extent if they were forced to make sure that nothing illegal is transmitted over their communication channels, is intrusive and potentially threatening to fundamental rights. A general surveillance tool based on DPI being used by the communications industry is not acceptable nor even desired by most ISPs. As identified by the European Court of Justice, although such tools make it possible to read all communications transmitted over the network, it comes at the price of a clear and obvious weakening of fundamental rights, such as freedom of expression, freedom to conduct a business, privacy and confidentiality of communications, and property and intellectual property.

The sense of the prohibition of general monitoring obligations resides precisely in this: by maintaining that ISPs do not have a duty to monitor their communications channels, and thus making them not strictly liable for omitting to engage in such control, legislators have been attempting to remove those legal and economic mechanisms that otherwise would justify such intrusive control of their networks. On the other hand, ISPs which decide to employ such tools, for example to throttle peer-to-peer file sharing, should be careful since control of and the ability to modify content could be the gateway to liability.