Gate Keeper or Trespasser? EU ISP Liability Regime and its Privacy Implications*

By LL.M. Branka Marusic

1. Introduction

The development of the internet brought numerous advantages to end users due to its services all over the world. The idea of availability of content and the instantaneous spread of ideas and concepts provided for a public arena in which end users could come together and reap the benefits of this interlinked world. However, a major problem that has arisen with this brave new world of digital freedom are the problems of piracy and intellectual property infringement. And with the advent of social network websites and reports of violability of governmental data retention systems to hacker attacks, the question of who is liable for privacy infringements online has come into the spotlight. In both these issues the question who should be deemed responsible for the breaches had arisen. Placing the responsibility often shifted from the infringers, internet service providers ('ISP') that either directly or indirectly facilitate the breach and the end user. The legislators often found practical to place responsibility on the ISPs with certain reservations that would be discussed below.

In the case of *Google Spain*,[1] a preliminary ruling of the Court of Justice of the European Union (the 'CJEU') confirmed that in the case of privacy it was both possible and legitimate for end users to request that links provided by search engines (which are in the nature ISPs) such as Google be removed under their 'right to be forgotten' where information is 'inaccurate, inadequate, irrelevant or excessive'[2] or even 'not kept up-to-date' or 'kept longer than necessary.' The basis of the applicant's argument was that his own right to privacy has been infringed upon due to the existence of a link to the information that concerned him and that this information was no longer relevant or accurate.[3] Es-

* The article has been peer reviewed.

[1] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja* [2014] (Not reported yet).

[2] Ibid [1] para. 94.

[3] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja* [2014] (Not reported yet) para 93; Article 12 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201, 31/07/2002 P. 0037–0047 (the 'ePrivacy Directive')*.

sentially, the responsibility was on the search engine to remove the damaging links and safeguard its right to privacy.

The CJEU ruled that issues pertaining to privacy were to be considered on a case-by-case basis and judged according to the principle of proportionally. The issue in *Google Spain* was a complaint made by a Spanish citizen Mario Costeja Gonzalez against Google. Mr Gonzalez demanded Google filter out his name from search queries linked to the repossession of his homes in a story first published in the Spanish newspaper La Vanguardia. Mr Gonzalez found that search results providing this information breached his fundamental right of privacy. Having considered the relevant principle and reasoning, the CJEU agreed with the applicant in this case. Ironically, Mr Gonzalez may have provided a 'right to be forgotten' to the online community, yet he will not be forgotten by that same community.

The CJEU decision concerning the 'right to be forgotten' metaphorically planted a seed that bore a bloom of reactions and effects. The parties negatively afflicted by the decision, and specifically Wikipedia, have dubbed the decision on the 'right to be forgotten' simply as 'censorship of truthful information' that 'threatens the organisation's mission to provide 'free access to the sum of all human knowledge' and that compromises human rights and freedom of expression.[4] As a response, the Wikimedia Foundation has also published statements online that Wikipedia will provide notices of all links to Wikipedia that are removed, when they are made aware of them.

In addition to Wikipedia, Google has also focused upon the inanity and operational *impossibility* of providing for the 'right to be forgotten' in line with the CJEU decision. For example, after the decision Google released an article that recorded their removal of links to Wikipedia pages under the 'right to be forgotten,' despite the fact that Wikipedia pages are open to constant editing and could simply be updated. Further, Google has highlighted in a response to regulators concerning their implementation of the 'right to be forgotten' that the mechanism is predominantly one-sided, as it is based on information provided by an applicant, which is often weak in efficacy and accuracy.

This case provides just one example of an infinite number of occasions in which parties such as end users, content owners and rights management organisations have sought to assign intermediaries/Internet Service Providers (ISPs) with liability for infringements perpetrated online. Internet actors often look to ISPs as the gatekeepers of the web and therefore the most suitable party to be held liable in relation to illegal online activity, whether it is in relation to economic *or* fundamental rights and interests. Accordingly, this article provides an overview of the ever-shifting notion of ISP liability in the online digital environment in light of the Google Spain decision, in a specific attempt to answer the following question: how far are we willing to affect the functioning of ISPs

[4] *http://www.theguardian.com/technology/2014/aug/06/wikipedia-censorship-right-to-be-forgotten-ruling* accessed on 2 December 2014.

through their liability for online activity in order to install order in an unruly digital arena?

2. ISP liability: Why and for What?

In the current state of the digital arena, it is well-established fact that illicit file sharing on the Internet is a major legal and economic concern for Member States within the EU.[5] This is so despite the fact of ongoing and extensive litigation, the use of technological protection measures and the development of new legislative measures to combat infringement.[6] As a result of this, interested parties seek to actively enforce their rights through new and effective online governance. But what exactly does governance entail in the context of the ever-evolving online digital environment? The *Working Group on Internet Governance* defines Internet Governance as '[t]he development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.'[7] This definition indicates that the online governance is a shared aim and emerging concept that must be apportioned between the parties that are both responsible, and yet importantly, also capable of governing actions. This definition also indicates that the perceived roles of involved parties, such as intermediaries, will be susceptible to continual change, redefinition and even reinvention as new online governance challenges continue to emerge.

In the current context, the question is how the role of intermediaries on the Internet should be redefined given the involvement of end users and consumers in illegal file sharing as well as privacy infringement. It should be noted that these intermediaries take different forms in an on line digital market. They can be in a form of different platforms that provide services, such as Spotify for on line music, they can be in a form of on line market place such as E-Bay, search engines such us Google or Bing, and regular web sites that provide information. The key common denominator is that the services are normally provided for remuneration (but not necessary), at a distance, by electronic means and at the individual request of a recipient of services (end users).

There have been several legislative acts on an EU level that placed the responsibility of data protection on ISPs, most notably the ePrivacy Directive and the Data Protection Directive.[8] However, the E-Commerce Directive[9] provides for safe harbour provisions in regards of the ISP liability. In case law of the CJEU, these safe harbour provisions have been applied to search engines in

[5] Adrienne Muir, 'Online Copyright Enforcement by Internet Service Providers,' 39 *Journal of Information Science* (2013) 256, 256.
[6] Ibid [5] p. 256.
[7] Section II, Working Group on Internet Governance, *Report from the Working Group on Internet, http://www.itu.int/wsis/docs2/pc3/html/off5/index.html* (2005, accessed January 1 2014).
[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23/11/1995 P. 0031–0050* (*the 'Data Protection Directive'*).

their capacity as ISPs and in regards to piracy and intellectual property rights infringement.

When we discuss the liability of ISPs, a distinction needs to be made between liability for breach of *economic rights* (that derive from intellectual property rights) and liability for breach of *fundamental rights* (fundamental human rights and freedoms). The view of different parties in relation to protection of these conceptually different rights and interests varies dramatically. It is well known that respect for economic component of intellectual property rights online is often lacking or entirely absent. The underlying problem in the digital arena is that, unlike physical market and physical property, the digital market and intellectual property often inspires an underlying end user perception that everything is accessible free of charge and is available for their use. This in turn causes a serious difficulty in the enforcement of the economic component of intellectual property rights. Such dysfunction can be explained by two particular issues, firstly, the end user expectation of 'free and on demand' content that is accessible online, and, secondly, the problem of facilitation of a framework of distribution of goods, services and content without the authorisation of the author or the intellectual property rights holder. However, when we consider fundamental rights linked to intellectual property (such as freedom of expression and privacy) the end users' perception of protection for these interests' shifts dramatically. Where fundamental rights are concerned, the end user demands protection and often views information that is directly linked to her or him as sensitive, or confidential and classified.

2.1 Modes of placing the liability for on line infringements. The task of placing liability on any particular actor in the digital environment is an onerous one for two main reasons, firstly, due to the persistent lack of recognition end users show for intellectual property rights online, and secondly, due to the sensitivity of applying measures where fundamental rights and freedoms may be encroached upon. A legislator can adopt several strategies, which are either to pursue individual infringers, the ISPs or both. The practical impossibility of pursuing individual infringers has led intellectual property rights stakeholders to vest efforts in placing responsibility with intermediaries.[10] Actors have previously targeted intermediaries responsible for the platforms that carried user-generated-content (the 'UGC'). However, the ability of intermediaries to be held liable here has been limited by the judicial interpretation of the safe harbour provisions for ISPs under the E-Commerce Directive.[11] In contrast, a general consensus has now de-

[9] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal C 178, 17.07.2000 (the 'E-Commerce Directive').

[10] Peter Danowsky: *The Enforcement of Copyright in a Borderless Online Environment: A Practitioner's View in Copyright in a Borderless Online Environment* (Axhamn (ed.), Norstedts juridik, 2012, p. 127–135.

veloped that ISPs are the best placed party, in both a theoretical and practical sense, to respond to online infringement via end user access to the internet.

In WIPO's review of the *Impact of the Internet on Intellectual Property*,[12] the issue was raised that by the very nature of digital networks, where work is transmitted, or made available to the public by multiple parties, an ISP should be held responsible where it '…is found to have engaged in unauthorized acts of reproduction or communication to the public, or if it is held responsible for contributing to or making possible the act of infringement by another.' Danowsky holds the more simple and practical view that it is simply '…fair and just that someone who can actually affect whether or not an infringement occurs bear responsibility for it.'[13] Both of these positions indicate that the perception of liability for ISPs is largely 'knowledge-based' or 'with-fault,' and that where knowledge or fault of infringement is present, an ISP should be required to take action.

In light of these views, two approaches exist for assigning this liability of an ISP in relation to intellectual property right infringement. They are characterized as either vertical or horizontal. The vertical approach is characteristic of intellectual property laws in the United States, where liability regimes are each individually applied to different areas of law.[14] In contrast, laws that are characteristic of the horizontal approach to liability are applicable to any form of infringement regardless of the relevant topic of law. This means that laws not only apply to copyright infringement, but also to other laws concerning matters such as privacy and defamation.[15] This approach is exemplified in the E-Commerce Directive.[16]

3. ISP Liability under the E-Commerce Directive

The E-Commerce Directive was adopted in 2000 in an attempt to both harmonise the internal market in relation to electronic commerce and further develop

[11] See: SABAM v Scarlet (C-70/10); SABAM V Netlog (C-360/10) 2 C.M.L.R. 18 and Scarlet v Sabam [2012] (C-70/10) E.T.M.R. 4, Joined cases C-236/08 to C-238/08, Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08) [2010] ECR I-02417, Case C-324/09, L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi [2011] ECR I-0000.

[12] Available at *http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap3.html#_ftn114* (Accessed 28 December 2013).

[13] Ibid [10], p. 128.

[14] *Role and responsibility of internet intermediaries in the field of copyright and related rights*, prepared by Lilian Edwards, Professor of E-Governance, University of Strathclyde, p. 7. available at *http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf* (Accessed 1 February 2015).

[15] *See*: ibid [10], WIPO article, also see "Liability," Issue Group Policy Paper: Final Draft, GBDe (August 3, 1999).

[16] Pablo Asbo Baistrocchi, 'Intermediary Service Providers in the EU Directive on Electronic Commerce,' 19 Santa Clara Computer & High Tech Law Journal 111, p. 117.

'information society services'[17] by providing enhanced legal certainty and clarity for consumers and stakeholders.[18] The key provisions in the current discussion are Articles 12 to 15 of the Directive. These articles provide for 'Informational Society Service Providers'[19] liability in the form of exclusions, or limitations, from liability that may arise at the national level. These liability exclusion provisions of the E-Commerce Directive have been widely incorporated into national legislation of Member States for both civil and criminal matters. In order to satisfy the requirements for exclusion from liability, an ISP must either qualify as a 'mere conduit'[20] or 'hosting provider,'[21] or only be involved in 'caching'[22] activity. Additionally, there is no general obligation to monitor the content that is stored and transmitted by the ISP under the aforementioned three categories. It should be noted that the safe harbour provisions only apply to ISPs when they are intermediaries of the information, and not the originators of the information. In this regard their contributory liability is negatively defined, meaning that there are situations where liability cannot be inferred. Furthermore, this is not an exclusive list of safe harbour provisions, and Member States can add to it. For example, Sweden in § 17 of the Swedish Law on E-Commerce[23] provides for a streaming safe harbour and Croatia in Article 19 of the Croatian E-Commerce Act[24] provides for a linking safe harbour.

Further to this, a positive responsibility to seek facts or circumstances indicating illegal activity cannot be placed on ISPs. Interestingly, in seeming contrast to Article 15, recital 48 of the E-Commerce Directive also introduces 'duties of care' that can be assigned to service providers that host information, '…which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities'.[25] Further, recital 47 also allows for a monitoring obligation in a specific case where injunctive actions are necessary. This issue was touched upon in the case *SABAM*,[26]

[17] Stefan Kulk and F. Z Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases,' 11 European Intellectual Property Law Review (2012) 791, p. 792.

[18] Patrick Van Eecke and Barbara Ooms, 'ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs,' Journal of Internet Law (2007) 3.

[19] 'Information Society Services' means any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. *See* Article 2a of Convention on Information and Legal Co-operation concerning "Information Society Services".

[20] ISPs that transmit information from one point on a network to another at the request of the recipient of the service or that simply provide access to a communication network.

[21] ISPs that store information provided by a recipient of a service.

[22] The automatic, intermediate and temporary storage of information for the sole purpose of making more efficient the onward transmission of that information.

[23] Lag om elektronisk handel och andra informationssamhällets tjänster [2002:562].

[24] Zakon o elektronièkoj trgovini ("Narodne novine", broj 173/03, 67/08, 36/09 i 130/11).

[25] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal C 178, 17.07.2000, p 1. Also see ibid [53], Patrick Van Eecke and Barbara Ooms, p 5.

[26] *SABAM v Scarlet* (C-70/10); *SABAM V Netlog* (C-360/10) 2 C.M.L.R. 18 and *Scarlet v Sabam* [2012] (C-70/10) E.T.M.R. 4.

where it was clarified that ISPs do not have a general obligation to monitor information, which is in line with Article 15 of the E-Commerce Directive. Specifically, CJEU stated that a requested injunction would require the ISP to actively monitor all of its customers' traffic, which would contravene the E-Commerce directive.

The CJEU case law on the interpretation of the E-Commerce Directive is based on the same notion noted above of 'control over content' for establishment of liability. Essentially, liability for breaches of economic rights of the intellectual property rights ('IPR') holder is placed on the ISPs that do not fall under the safe harbour provisions of the E-Commerce Directive. In the case law of the CJEU, most notably *Google France*[27] and *L'Oréal vs. E-Bay*,[28] search engines such as Google and sale and purchase websites such as eBay were identified as intermediaries, and not originators of information, thus falling under the safe harbour provisions. In the case law of Member States, the liability for breaches of economic rights of IPR holders has been excluded for ISPs such as YouTube in Italy[29] and Spain,[30] as well as Google in France.[31]

However, Member States have not only considered the applicability of safe harbour provisions in matters concerning liability for breaches of economic rights of IPR holders, but also breaches of fundamental rights. Most notably, Italy recognised Wikipedia[32] as a hosting service and not liable when it comes to defamation. Similarly, Google[33] was found not liable for privacy infringement.

3.1 Control over content vs. strict liability. Up until the case of *Google Spain*,[34] the legislative acts and case law of the CJEU have determined that the notion of liability of the ISPs, such as Google, is interlinked with the possibility of the ISPs to control the content that was made available through them. The control over content liability has been established in the EU Member States jurisdictions in various models. These models vary from targeting the end users in France through the 'three strikes and you are out' policy, 'take the ISPs to Court' pol-

[27] Joined cases C-236/08 to C-238/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08)* [2010] ECR I-02417.

[28] Case C-324/09, *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi* [2011] ECR I-0000.

[29] Tribunale ordinario di Torino, causa n.r.g. 15128/2014, Delta TV programs srl c/a Google Ireland Holdings, Google Inc, YouTube, 23 January 2014.

[30] Madrid Civil Court of Appeal, case no 505/2012, Gestevision Telecinco c/a YouTube LLC, 14 January 2014.

[31] Cour de cassation, chambre commerciale, Audience publique du mardi 29 janvier 2013, N° de pourvoi: 11-21011 11-24713.

[32] Tribunale ordinario di Roma, causa civile di primo grado n. 705727/09, Angelucci c/a Wikimedia Foundation Inc. Italia, 4 July 2014.

[33] Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – 3 febbraio 2014, n. 5107/2014.

[34] Ibid [1].

icy in Germany, 'graduate response and site blocking tactics' in the UK or 'notice and take down procedures' in Italy. The safe harbour provisions of the E-Commerce Directive implemented in the national law of EU Member States provided for a balance that took into consideration the fact that the ISPs' nature of business model would not be able to control the content made available through them. This model of safe harbours in liability has been primarily tested within the ambit of liability for breaches of economic rights, where the content that was shared via the ISPs was found to be in breach of intellectual property rights. Member States such as Italy[35] found it logical to extend this model of liability to breaches of fundamental rights as well.

3.1.1 Liability for breaches of fundamental rights. In order to discuss the liability for breaches of fundamental rights in the EU, we must first observe the legislative framework that guarantees the observance of the fundamental rights. As a general framework, the fundamental rights on the territory of the EU are protected in three different ways. Firstly, they are protected through national laws, most notably individual constitutions of Member States. Secondly, they are protected on a European-wide level through the European Convention on Human Rights,[36] and lastly on the EU level through the Charter of Fundamental Rights.[37] The relationship between the three ways of protection can be portrayed as complicated; however, it can be stated that the national laws harmonise themselves both with the ECHR and the Charter, and that the ECHR and the Charter are in accordance and respect of each other's case law.[38]

On an EU level, with the legislative framework that was tailored to address liability for breaches of economic rights of the IPR holder, soon emerged the need to address issues of fundamental rights. Although both the European Court of Human Rights (the "ECtHR") and the CJEU flirted with the balancing act of a clash between economic and fundamental rights, they never dared to give a definite answer weather which one would take precedent, under which circumstances and under what criteria, and left these questions to be dealt with on the national level of each Member State.[39] These decisions created ambiguity and legal uncertainty when it came to a way to deal with the rights and obligations of IPR holders, the ISPs' and the end users. Due to the

[35] *See*: Tribunale ordinario di Roma, causa civile di primo grado n. 705727/09, Angelucci c/a Wikimedia Foundation Inc. Italia, 4 July 2014. and Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – 3 febbraio 2014, n. 5107/2014.

[36] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ.T.S. No. 5; 213 U.N.T.S. 221 (the 'ECHR').

[37] Charter of Fundamental Rights of the European Union, 30.3.2010., OJ C83, pp. 389–403 (the 'Charter').

[38] *See*: Case 4-73, *Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*, ECR [1974], 491, par. 13; C-260/89 *ERT* (1991) ECR I-02925, para. 44; *Bosphorus Hava Yollari Turizm v. Ireland*, App. No. 45036/98 (Eur. Ct. H. R. 30 June 2005) paras. 7376.

[39] *See:* Case C-275/06, *Promusicae vs. Telefónica*, 29 January 2008, OJ C 64, 08.03.2008; ECHR 10 January 2013, *Ashby Donald and others* v *France*, no. 36769/08 and ECHR 19 February 2013, *Neij and Sunde Kolmisoppi* v *Sweden*, no. 40397/12.

factor of uncertainty, rules that were applied for liability for breaches of economic rights of IPR holders were analogously applied to liability for breaches of fundamental rights by the Member States. Both the ECtHR and the CJEU avoided giving a clear-cut answer and any direct guidance to the Member States on how to proceed with this balancing act.

3.1.2 Regulation of liability for privacy breaches on an European level. The national laws of Member States point towards two emerging issues in the online world when it comes to privacy: data retention and disclosure of information. The notion of privacy and its scope and subject matter, and the mechanism of protection vary in different Member States.

Regarding data retention, that issue was traditionally observed through the lenses of state powers and what the borders of state intervention in privacy issues are.[40] On an EU wide level, the primary view of the national state being the only actor involved in data retention and respect of privacy, has changed. The new identified actors in the digital arena consist of private controllers of data flows and information, as well as the ISPs. The CJEU through its case law tried to provide a glimpse of where liability lies (or should not lie) when other actors are involved. The relevant issue touched upon was the filtering system in the case *SABAM*,[41] where it was stated that the obligation to place filtering systems in a form of preventive monitoring would require active observation of all electronic communications conducted on the network and consequently, would encompass all information to be transmitted to and from all customers using that network. It was seen that this in turn could have a negative effect on fundamental rights. However, the CJEU did not go any deeper into analysis on this issue.

In regards of the second emerging issue, the disclosure of information online, whether executed by individuals,[42] journalists,[43] the state,[44] or whether information is to be disclosed for the purposes of fighting copyright infringement,[45] the CJEU, as well as the ECtHR,[46] did not provide for a clear answer where is the line between information that should be made available to the general public and the right of privacy and held that this balancing act should be done by national courts.

However, the ECtHR and the CJEU as well as the EU Member States used the notion of control over content in order to test the boundaries of liability. It was found to be logical that the entity that is to be held responsible both for the liability for breaches of economic rights of the IPR holder and fundamental

[40] ECHR 18 July 2013 M. K. v France no. 19522/09; ECHR 29 April 2013 *M.M. v United Kingdom* no. 24029/07.
[41] Ibid. [26].
[42] C-101/01 *Bodil Lindqvist*, ECR [2003]Page I-12971.
[43] C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy ECR [2008]Page I-09831.
[44] C-524/06 Heinz Huber v Bundesrepublik Deutschland ECR [2008] Page I-09705.
[45] C-461/10 Bonnier Audio AB and Others v Perfect Communication Sweden AB ECR [2012].
[46] ECHR December 2008 *K.U. v. Finland* 2 no. 2872/02.

rights should somehow control the infringing content. How this control occurs and what the levels of it has always left to be tested on national levels. The CJEU and the ECtHR never went into analysis of the conditions or guidance as to how this should be carried out, except stating that notions such as proportionality of measures should be taken into consideration by national courts and legislators.

On an ECtHR level, the recent development has been seen as troubling. On the one hand, in *Delfi*[47] the ECtHR stated that ISPs are liable for anonymous defamation. With this, the ECtHR widened the liability for breaches of fundamental rights by taking into account the technical measures that might be employed in order to control the content provided by users of the ISPs. Furthermore, it was reluctant to employ the safe harbour provisions of the E-Commerce Directive, and automatically dismissed them as irrelevant. On the other hand, the ECtHR stated that countries have a wide margin of appreciation when deciding whether use of fundamental rights can derogate liability for breaches of economic rights of the IPR holder (more specifically whether freedom of expression trumps copyright).[48] This development only leads to more caution and self-censoring because the ISPs have liability for breaches of fundamental rights if they can control the technical means through which content is disbursed. Furthermore, the uncertainty in the realm of liability for breaches of economic rights of the IPR holder can be seen through the lack of definition of what the new access point of derogation of liability for breaches of economic rights through use of fundamental rights entails.

The role of the ISPs is to provide Information Society Services that are normally provided for remuneration (but do not need to be), at a distance, by electronic means and at the individual request of a recipient of services.[49] This includes websites, search engines, forums, social networks, etc. The portrait of ISPs liability so far remains unclear, ambiguous and somewhat unorderly. The only common consensus in both liability for breaches of economic rights of the IPR holder and fundamental rights is that if the ISPs exert some sort of control over the content they are liable for it. The liability for breaches of economic rights is placed on the ISPs that do not fall under the safe harbour provisions of the E-Commerce Directive, while those that are liable for fundamental rights breaches are ISPs that have the option to control the visibility of content (i.e. the ones that can have a decisive role in what appears on or through their services).

3.1.3 Google Spain's introduction of strict liability. The CJEU *Google Spain* judgement sets a new precedent regarding the notion of safe harbour provisions, and shifts the current trend of recognition of the latter in both economic rights of the IPR holder and fundamental rights cases. The trend of case law, both at

[47] ECHR *Delfi AS v. Estonia*, 10 October 2013 no. 64569/09.
[48] ECHR 10 January 2013, *Ashby Donald and others* v *France*, no. 36769/08 and ECHR 19 February 2013, *Neij and Sunde Kolmisoppi* v *Sweden*, no. 40397/12.
[49] Article 2 (a) of the E-Commerce Directive.

CJEU and on Member States level, is to view search engines as a 'mere' or 'neutral' hosting providers because they play a passive role in the management of online content and have neither knowledge nor control over the information which is transmitted or stored. However, in *Google Spain* it was decided that if the content that is displayed through search results concerns personal data a search engine will be regarded as a 'controller' responsible for the 'processing of personal data', according to the definitions provided under the Data Protection Directive. It is irrelevant if the search engine has any actual knowledge of the type of content (personal or otherwise) that is displayed through search results. This view displaces the previous notion for ISPs that 'control over content' or that the active/passive dichotomy will establish liability. It also gives rise to a legal confusion and general inanity in relation to the way in which the search engine is to fulfil its functions. In addition, it poses the question whether the liability for privacy infringement should be judged under the current mechanisms of Member States for liability for breaches of economic rights of the IPR holder.

Google Spain judgment concerned a Spanish citizen, Mr Gonzalez, who lodged a complaint in 2010 against a Spanish newspaper with the national Data Protection Agency and against Google Spain and Google Inc. He complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant. He requested, first, that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared; and second, that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results. Essentially, he requested to 'be forgotten'. The CJEU clarified three issues, first was the territorial applicability of EU rules, in which it stated that even if the physical server of a company processing data is located outside Europe, EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State which promotes the selling of advertising space offered by the search engine.[50] Secondly, was the applicability of EU data protection rules to a search engine, in which it stated that search engines are controllers of personal data, and therefore the EU data protection rules apply to them.[51] The CJEU went further and specified[52] the mechanism of data retention/data accessibility by identifying two levels of privacy. The first level refers to the publisher of the websites that contain information (in the case of *Google Spain* it was newspapers and in the example from the introduction part that would be Wikipedia). By way of technology such as exclusion protocols 'robot.txt' or codes such as 'noindex' or 'noarchive', they have an option to exclude the information to be searchable through search engines. The second

[50] Ibid. [1] para. 55.
[51] Ibid. [1] para. 34.
[52] Ibid. [1] para. 39.

level is the search engine. Here the CJEU states that if the publishers of websites do not exclude the information, this does not release the search engines from their responsibility to remedy breaches of privacy (liability for breach of fundamental rights). On the contrary, the liability for breach of fundamental rights rests on the search engines, and it is their responsibility to remedy this breach. Thirdly, the CJEU concluded that there exist a 'right to be forgotten' where information is 'inaccurate, inadequate, irrelevant or excessive'[53] or even 'not kept up-to-date' or 'kept longer than necessary.'

This is problematic on several levels. Firstly, the ISPs that fall within the safe harbour provisions of the E-Commerce Directive when it comes to liability for breaches of economic rights of the IPR holder fall outside of their scope when it comes to privacy issues. This contradicts the notion of 'control over content' for establishment of liability, both on the EU and Member States level of application of safe harbour provisions on liability for breaches of economic rights of the IPR holder and fundamental rights. Furthermore, this also contravenes the ECtHR case law on the interpretation of the functioning of fundamental rights on the ISPs.

Secondly, it creates a legal confusion, where ISPs who are granted the safe harbours when it comes to liability for breaches of economic rights of the IPR holder, need to exercise the 'right to be forgotten' not only on themselves, but on websites that they are not publishers of. To place it in the context of Wikipedia, when Google receives a notice-to-take-down a web link, this web link disappears from Wikipedia, thus directly influencing the website. With this, Google has a double burden of preserving privacy (first and second level, as described in para 39 of the *Google Spain* judgment) and has a censorship function, because with this action, it deletes content without prior notice or authorisation from a publisher of a website (in the example of Wikipedia).

4. Conclusion

The initial liability for the breach of economic rights of the IPR holder of the ISPs has evolved into the liability for breaches of fundamental rights, firstly in the form of preservation of the freedom of expression in the digital arena, and currently in the form of preservation of privacy.

As illustrated in the analysis of ISP liability and the current state of laws within the EU the freedom that minimum harmonization rules in the EU Directives provide to Member States for the application and enforcement of ISP liability has led to a rather chaotic situation. This in turn has led to a divergent development in the approaches of the CJEU, the ECtHR and the Member States in defining liability for breach of economic rights of the IPR holder and fundamental rights of the ISPs and consequently applying safe harbour provisions to such liability. Within Europe, approaches continue to shift and change as multiple industry stakeholders attempt to protect and preserve their interests in the online digital environment. The result of this is that industry stakeholders

[53] Ibid. [1] para. 94.

and ISPs are privately acting to protect their own rights in the current setting, either through private agreements, settling negotiations out of court or self-censuring by removing content on request. The simple point here is that an ISP may not be liable for infringement of the economic rights of the IPR holder, but is nevertheless liable for privacy infringement. By this, *Google Spain* demonstrated the trend of how liability of ISPs is becoming wider in scope, yet the definitions of what liability entails are becoming more blurred. These developments can be problematic for parties that do not hold leverage against more powerful stakeholders and ISPs that are left without clear definitions of what is acceptable and legal conduct. This is even more so given the margin of appreciation that both the ECtHR and the CJEU had left to the Member States when implementing and enforcing both copyright-related laws and the laws pertaining to fundamental rights and freedoms.

Coherent policy that apportions appropriate responsibility for ISPs by, for example, making the original safe harbour provisions of the E-Commerce Directive effective once again is required. Moreover, clear definitions on when they apply are paramount. This is required both via legislation and through the approach of the courts.

The current state of the market which targets ISPs and places the liability on them both for their actions, actions of third party websites and the actions of their users creates a situation where legal certainty is undermined. The ISPs' current actions taken to shield themselves from this uncertainty in a form of self-regulating measures only lead to restrictions in the economic and fundamental rights arenas. Commercially, these measures create additional financial burden for the ISPs, diminishing their ability to operate effectively. This in turn makes them less attractive businesses for the end users to approach and use their services. In the fundamental rights arena, the end users are also not provided with any legal certainty in regard to the protection of their fundamental rights and interests because there is no balancing act between them.

Currently, there is a dire need in the market to make the safe harbour provisions effective. The suggestion is that there should be a uniformed application throughout Europe for both the liability for breach of economic rights of the IPR holder and fundamental rights due to the fact that this policy brings about legal clarity and certainty in everyday operations of the ISPs. The evolving state of ISP liability helps to illustrate that multiple interpretations and applications of the EU Directives are possible. Member States are relatively free to implement and enforce the Directives to varying degrees. Van Eecke and Oms[54] rightly note that in the current context, where ambiguity exists for the implementation of the EU Directives, and consequently for the legal liability of intermediary actors, ISPs will embark upon greater self-regulation for the sake of preserving their own rights and interests. As the industry and state stakeholders attempt to assign a greater responsibility for ISPs to execute intensified monitoring and

[54] Patrick Van Eeecke & Barbara Ooms, 'ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs,' *Journal of Internet Law* (October 2007).

data collection activities for the purposes of enforcing liability for breaches of economic and fundamental rights, the application of safe harbour provisions is made all the more problematic. Furthermore, these self-regulating actions of ISPs can have an illegitimate effect upon the fundamental rights and freedoms of individual end users due to the absence of leverage the parties have against more powerful stakeholders. The uniform application of safe harbour provisions would provide greater clarity for all the parties concerned from the legal limbo they are currently attempting to operate within online.