Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe

by **Bart van der Sloot***

Abstract: In Europe, roughly three regimes apply to the liability of Internet intermediaries for privacy violations conducted by users through their network. These are: the e-Commerce Directive, which, under certain conditions, excludes them from liability; the Data Protection Directive, which imposes a number of duties and responsibilities on providers processing personal data; and the freedom of expression, contained inter alia in the ECHR, which, under certain conditions, grants Internet providers several privileges and freedoms. Each doctrine has its own field of application, but they also have partial overlap. In practice, this creates legal inequality and uncertainty, especially with regard to providers that host online platforms and process User Generated Content.

Keywords: liability; intermediaries; privacy violations; ECHR; freedom of expression; data protection

Recommended citation: Bart van der Sloot, Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe, 6 (2015) JIPITEC 211 para 1.

A. Introduction

1 When Internet companies and private parties started to offer Internet services in the 1980s, there was already discussion concerning the position of Internet intermediaries. Initially, the provider was often seen as the digital equivalent of a postal company, which had neither knowledge of nor control over the post that was delivered by it and therefore could not, in principle, be held liable for any illegal content. At that time however, there existed two separate doctrines regarding third party liability for copyright infringements in the United States, where the Internet experienced its initial growth. "Vicarious liability" entailed that a third party could be held liable for infringing activities if it had the right and ability to control over and gained financial profits from the activity, and "contributory liability", which regarded third parties that had knowledge of and contributed to the infringing activity.[1] These doctrines were gradually also applied to Internet service providers. This meant that if an Internet intermediary wanted to avoid liability for, for example, copyright infringements by its users, the intermediary would have to prove that it did not know of the infringing nature of the material, that it did not contribute in any way to the infringement and that it had not received any financial gain from the infringement.[2]

2 This jurisprudential doctrine was subsequently further developed in the US Digital Millennium Copyright Act (DMCA) of 1998, which makes a distinction between (1) providers that offer access to networks and data transmission via these networks (access providers/mere conduits), (2) providers temporarily storing material on their server (caching providers), (3) providers that store information or host websites (hosting providers) and (4) providers that offer links to websites or make content searchable (search engine providers).[3] The European Union (EU) has a regulation similar to the DMCA,[4]

1 A. Strowel, 'Peer-to-Peer file sharing and secondary liability in Copyright Law', Cheltenham, Edward Elgar Publishing, 2009.

2 M. B. Nimmer & D. Nimmer, 'Nimmer on copyright: a treatise on the law of literary, musical and artistic property, and the protection of ideas', New York: Bender, 1994.

3 Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998), para. 512.

4 See for a good comparison: M. Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems', Columbia Journal of Law &

laid down in the e-Commerce Directive 2000.[5] The rules therein contained form the general basis for the exclusion of liability of Internet intermediaries under European law (so called safe harbors). Although this regime applies to virtually all offenses, data protection issues are explicitly excluded.[6] In such cases, the Data Protection Directive[7] applies. There is a third regime that is increasingly applied as well, namely when an Internet intermediary relies on the freedom of expression to protect its own interests, for example under the European Convention on Human Rights (ECHR).

3 It should be borne in mind that in the early days, Internet intermediaries were predominantly of a passive nature, and that the e-Commerce Directive is written for providers that transmit or store material on behalf of users only. In the modern Internet landscape however, providers have become much more active, for example by providing the platform on which information is shared by users, by indexing this information, by making it searchable and by publishing and distributing the information over the Internet. Examples of active Internet intermediaries are platforms such as Facebook, video services such as Youtube, digital markets such as eBay and modern media such as WikiLeaks or news sites (partially or primarily) based on stories, contributions and comments written by users. In these examples, the content is still provided by the users, but the role of the Internet intermediary is no longer merely to transmit, store or publish the material on behalf of the user – rather it fulfils an active role in the organization and functioning of the websites and platforms. The question thus becomes what position these providers have with regard to material of an infringing nature uploaded by their users.

4 Recently, the Court of Justice (ECJ) ruled in its Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González verdict (hereafter: Google Spain) that Google may be required to block or delink certain information from other website in its search engine in order to respect the data subject's right to be forgotten.[8] The ECJ has also held that the obligation to monitor and store all Internet traffic, contained in the Data Retention Directive, is invalid and violates the rights to privacy and data protection.[9] In Delfi v. Estonia, the European Court of Human Rights (ECtHR) in 2013 and the Grand Chamber of the ECtHR in 2015 ruled that online news sites that facilitate user reactions can invoke the right to freedom of expression, but can also be held liable for user comments that harm third party interests.[10] The Council of Europe (CoE), in 2011, developed a new vision on modern media, proposing inter alia to apply the classic protection of journalists to bloggers and other new media.[11] In addition, there are advanced plans in the EU to introduce the General Data Protection Regulation, which will radically change the legal data protection regime laid down in the current Data Protection Directive.[12] Finally, for years now, there has been a discussion concerning the possible revision of the e-Commerce Directive, precisely as regards to the liability regime for Internet intermediaries, in which respect the European Commission in 2010 initiated a public consultation[13] and in 2012 launched a special consultation on hosting providers.[14]

5 This contribution will explain and analyze the three legal regimes in Europe that are applicable to Internet intermediaries, giving special attention to recent developments and case law. Section B discusses the liability regime under the e-Commerce Directive, the relevant case law of the ECJ and the plans to amend the directive. Section C discusses the regime under the Data Protection Directive, the relevant case law of the ECJ, including the Google Spain case, and the possible changes resulting from the pending General Data Protection Regulation. Section D discusses the doctrine on the freedom

Arts, vol. 32. no. 4, 2009.

5 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 or the e-Commerce Directive).

6 There are however authors that have rejected a literal reading of this provision. See among others: G. Sartor, "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?' International Data Privacy Law 2013-3.

7 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 (Data Protection Directive).

8 Court of Justice, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, case C131/12, 13 May 2014.

9 Court of Justice, Digital Rights Ireland Ltd (C293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C594/12), Michael Seitlinger, Christof Tschohl and others, cases C293/12 and C594/12, 08 April 2014.

10 European Court of Human Rights, Delfi AS v. Estonia, appl. no. 64569/09, 10 October 2013. European Court of Human Rights, Delfi AS v. Estonia, appl.no. 64569/09, 16 June 2015.

11 Committee of Ministers, 'A new notion of media', CM/Rec(2011)7, 21 September 2011.

12 In this contribution, for reasons of conciseness and clarity, reference shall be made only to the original proposal by the Commission. Commission, Proposal for a General Data Protection Regulation, COM(2012)11final, 25 January 2012.

13 http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

14 http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-Internet_en.htm.

of expression enshrined in Article 10 ECHR, the relevant case law of the ECtHR, including the case of Delfi v. Estonia, and the recommendation of the CoE. Finally, section E will provide a conclusion and an overview of the three regimes. This contribution will focus specifically on the position of hosting providers and active Internet intermediaries, as active intermediaries are increasingly dominant in the modern Internet environment, but their legal position is often vague and unclear.[15]

B. E-Commerce Directive

6 The e-Commerce Directive regulates a variety of different topics, including the liability of Internet intermediaries, providing so called safe harbors. A distinction is made between three types of services offered by providers. Firstly, Article 12 specifies that an access provider is not liable for the information transmitted, on the condition that the provider (a) does not initiate the transmission, (b) does not select the receiver of the transmission and (c) does not select or modify the information contained in the transmission. These providers are excluded from liability and have very limited additional responsibilities as long as they remain passive. Secondly, Article 13 regards providers engaged with caching. This provision has been of little importance so far and will therefore remain undiscussed in this contribution. Finally, Article 14 holds that a hosting provider is not liable for the information stored, provided that (a) the provider does not have actual knowledge of the illegal nature of the activity or information and, as regards to claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent and (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[16]

7 In addition, Article 15 provides that Member States may not impose a general obligation on intermediaries to monitor the information that they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. In the cases of Scarlet v. Sabam and Sabam v. Netlog,[17] the ECJ held inter alia that the e-Commerce Directive, read in conjunction with other directives, precludes "a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering information which is stored on its servers by its service users, which applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense and for an unlimited period, which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright."[18]

8 Remarkably, the e-Commerce Directive, unlike the DMCA, contains no specific provision for search engines. However, Article 21 states, among others, that the report on the implementation of the Directive should examine whether proposals ought to be made to amend the Directive in order to include rules on the liability of search engines. Meanwhile, the ECJ ruled in Google v. Louis Vuitton that Google's advertising service, which is provided in conjunction with its search engine, may fall within the scope of Article 14 since that provision must "be interpreted as meaning that the rule laid down therein applies to an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned."[19] It is not unreasonable to argue that the search function itself, under certain conditions, may also fall under the regime of Article 14.[20]

9 The question is, however, whether active Internet

15 See further: N. van Eijk (et al.), 'Moving Towards Balance: A study into duties of care on the Internet', http://www.ivir.nl/publicaties/download/679.

16 See also consideration 42 e-Commerce Directive. Whether this recital applies to Article 14 e-Commerce Directive is a matter of debate.

17 Court of Justice, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), intervening parties: Belgian Entertainment Association Video ASBL (BEA Video), Belgian Entertainment Association Music ASBL (BEA Music), Internet Service Provider Association ASBL (ISPA), case C-70/10, 24 November 2011. Court of Justice, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, case C360/10, 16 February 2012. See further: S. Kulk and F. Borgesius, 'Filtering for copyright enforcement in Europe after the Sabam cases', European Intellectual Property Review, Vol. 34 No. 11, 2012.

18 SABAM/Netlog, para. 53.

19 Court of Justice, Google France SARL, Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA, Luteciel SARL (C-237/08), and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), cases C-236/08, C-237/08 and C-238/08, 23 March 2010, para. 120.

20 See more in general: J. van Hoboken, 'Search engine freedom: on the implications of the right to freedom of expression for the legal governance of web search engines', Kluwer Law International, Alphen aan den Rijn, 2012.

intermediaries (such as s Facebook, Ebay, Youtube and news sites that run on User Generated Content) can also rely on Article 14. Of course, this will not be the case with, for example, news sites that publish their own material, written by their own employees on their own website.[21] They will be regarded as publishers, not as Internet providers. However, the question is more difficult to answer with respect to intermediaries such as Facebook, Ebay, Youtube and news sites that run on User Generated Content. The ECJ appears to have answered this question affirmatively in its L'Oreal v. Ebay ruling, which focused on illegal content posted by users on Ebay. The Court held in respect of Ebay that "the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31."[22] However, at the same time, it cannot "rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31."[23]

10 The phrase "diligent economic operator" causes a new problem. As active Internet intermediaries have a greater influence on and control over the websites than traditional hosting providers, it is generally assumed that active intermediaries also have a broader duty of care to ensure that their sites and platforms remain free of infringing material, for example, by monitoring their sites, by installing filter systems or by appointing system administrators. A study from 2010 hinted towards exactly this potential vicious circle. "Checking Internet traffic for [enforcement purposes] is not effective, and it is technically unfeasible. A formal duty of care would lead to excessive intervention by Internet service providers and possibly could escalate in the creation of further duties of care in other fields. Intervention with regard to illegal content in general might be next and would result in disproportionate restrictions on (future) economic activities on the Internet."[24] Consequently, duties of care may create a Catch-22 situation.[25] Since providers are more directly involved in the design and the layout of the websites, they have a broader duty of care; the broader duty of care implies that they should exercise additional control over the content submitted by users. However, this will create a situation in which they have an even greater involvement in and control over the platform or service, which again could entail an even broader obligation to monitor, filter and control content. This is a spiral to which there is no logical end. In practice, this issue creates much legal uncertainty, as national regulators and courts differ in their approach to this topic.[26]

11 As an example a Dutch case may be referred to, in which a file sharing site did filter pornography and viruses, but did not filter with respect to possibly copyright infringing material. The judge concluded that the site, Mininova, was liable for this content because it had the capacity and the means to control the site on illegal content, but refused to do so with respect to content infringing on intellectual property.[27] This means that from the capacity to control, a duty of further control may be derived.[28] This is partly due to the fact that Europe lacks a clear Good Samaritan clause, such as, inter alia, contained in the Communications Decency Act of the United States. 47 U.S. Code § 230, on the protection for private blocking and screening of offensive material, sub C, on the protection for "Good Samaritan" blocking and screening of offensive material, provides: "(1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of — (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)."[29]

21 See Art. 14 para. 2 e-Commerce Directive and Court of Justice, Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis, case C291/13, 11 September 2014.

22 Court of Justice, 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, case C324/09, 12 July 2011, para. 115.

23 L'Oréal/eBay, para. 124. See further: B. Clark, B. and M. Schubert, 'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oréal v eBay', Journal of Intellectual Property Law & Practice, Vol. 6 No. 12, 2011.

24 http://www.ivir.nl/publicaties/download/679.

25 J. Heller, 'Catch-22: a novel', New York, Simon and Schuster, 1961.

26 See also: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

27 ECLI:NL:RBUTR:2009:BJ6008.

28 See further: http://www.ivir.nl/publicaties/download/999.

29 https://www.law.cornell.edu/uscode/text/47/230.

12 In connection to this, mention should be made of the former plans to revise the system of liability under the e-Commerce Directive with regard to active Internet intermediaries and search engines. Both in 2003[30] and in 2008,[31] reports were issued, but both were very reticent about making actual proposals regarding effective changes to the liability regime. In 2010, the European Commission launched a public consultation on a possible revision, and the report, among other conclusions, states: "National jurisprudence on hyperlinking is very fragmented. A UK court considered it to be a mere conduit activity (art 12 ECD), a German court considered it to be a form of hosting (art 14 ECD), while a Belgian court considered that the ECD was not relevant for hyperlinking activities. Spain and Portugal have extended the liability exemption to hyperlinking and search engine activities."[32] This is just one example of the diversity of and imparity between the different national approaches to Internet liability. However, many respondents saw no benefit in changing the current protection regime. Reportedly, ISPs were afraid of further obligations and responsibilities; Intellectual Property organizations for a greater role for consumer rights; consumer groups for excessive lobbying by the industry, etc. For now, the current regime remains unaltered and it is left mainly to national courts and authorities to interpret the liability regime and apply it to new developments.

13 Finally, a noteworthy point regarding the application of the e-Commerce Directive to data protection matters. It follows from Article 1 paragraph 5 sub b, that the safe harbors do not apply to questions relating to information society services covered by the Data Protection Directive and the e-Privacy Directive.[33] Recital 40 of the e-Commerce Directive states that the existence of different regimes in respect of civil and criminal liability in the different countries distorts the internal market, which the directive would like to end by harmonization. The recital continues: "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 [the Data Protection Directive] and 97/66/EC [the predecessor of the e-Privacy Directive]." These are notoriously vague statements. For example, do they mean that the e-Commerce Directive could apply to data protection issues, but should not lead to a lower level of protection, or that the e-Commerce Directive simply does not apply to data protection issues at all?

14 The ECJ case law demonstrates that a distinction should be made between three types of cases. First, cases in which intermediaries are held liable for an infringement committed by a user through its network, for example, an intellectual property right - the e-Commerce Directive is applicable. Second, cases in which intermediaries are held liable for an infringement, committed by a user via its network, of a person's right to data protection - the Data Protection Directive is applicable. Third, cases in which an infringement of an intellectual property right has been initiated by a user and an Internet service provider is asked to provide the name and address of the user (that is to provide personal data) or to effectuate a monitoring system - both directives apply. In such cases, the ECJ will assess the case by relying on various directives, such as the e-Commerce Directive, the directives on data protection and the directives regarding the protection of intellectual property. For example, this was the case in the aforementioned matter of Scarlet v. Sabam, regarding the potential monitoring obligation imposed on an Internet intermediary.[34]

15 As an illustration, reference can also be made to the case of Promusicae v. Telefonica, which concerned the request for obtaining the names and addresses of users of Telefonica, whom were suspected of having used the KaZaA P2P network.[35] When the case went to court, Telefonica objected and argued that it could only provide the data in the context of criminal proceedings or in the case that it would be necessary to safeguard public order and national security, but not in the context of civil proceedings or as an interim measure prior to such proceedings. The question of the Spanish court to the ECJ was whether it was obliged to rule that Telefonica was obliged to provide the personal data of their customers. The Court held that the e-Commerce Directive, two directives regarding the protection of intellectual property,[36] and the e-Privacy Directive

30 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0702&from=EN.

31 http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

32 http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

33 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 or the e-Privacy Directive). Directive 97/66/EC has been replaced by Directive 2002/58/EC and the references to the first directive must be read as a reference to the second directive.

34 See further: Court of Justice, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, case C-557/07, 19 February 2009.

35 See also: C. Angelopoulos, 'Sketching the outline of a ghost: the fair balance between copyright and fundamental rights in intermediary third party liability', info, Vol. 17 Iss 6, 2015. X. Groussot, 'Rock the KaZaA: another clash of fundamental rights', Common Market Law Review, Vol. 45 No. 6, 2008.

36 Directive 2001/29/EC of the European Parliament and of the

had to be read in conjunction with each other and concluded that they "do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings."[37] How the balance between the different interests should be made depends on the circumstances of the case. Consequently, in the Promusicae v. Telefonica case, the ECJ refrained from providing a standard line of interpretation.[38]

C. The Data Protection Directive

16 The previous paragraph discussed the rules regarding the liability of Internet intermediaries with respect to infringements other than on the right to data protection. It also discussed the situation in which the right of users' data protection and the right to intellectual property of third parties clash. This section will analyze cases in which Internet intermediaries may be held liable for infringements on the right to data protection of third parties, conducted by their users through their networks. The Data Protection Directive generally applies when four criteria are met: (1) personal data, (2) are processed, (3) by a controller and (4) the territoriality principle applies. (1) Any data is personal data when a person could possibly be identified through it; importantly, "personal data" does not only revolve around private or privacy-sensitive data.[39] General and public information that can identify someone, such the phrase (indicating a person), "the man next to the lamppost", may already qualify as personal data.[40] Even if data at a given point in time does not identify anyone, but may do so over the course of time, for example by using advanced identification techniques, they will be considered "personal data". Consequently, ISPs will typically process personal data, as in almost every message, in every comment and on every website, personal data is contained.[41] (4) Additionally, the element of territoriality will usually be met, but this will not be discussed in depth in this contribution.[42]

17 (2) When something is done with personal data, it almost always falls under the legal definition of "processing", whether it denotes storing, publishing, distributing, blocking or even deleting data – it is all considered to be "processing".[43] Only the pure transmission of information provided by a user over a network will usually not fall under its scope. Consequently, access providers are in principle excluded from upholding the rights and duties under the Data Protection Directive.[44] Finally, there must be (3) a controller. The controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The controller is contrasted to the "processor", which is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.45 It follows, inter alia, that purely passive hosting providers, that neither determine the means nor the purpose of the data processing, will in principle not be considered the controller, but the processor of personal data. Therefore, they are not responsible for upholding the rights and duties under the Directive, the controller is. "An ISP providing hosting services is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If however, the ISP further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing."[46]

18 To this extent, the regime with regard to the responsibilities of Internet intermediaries under the Data Protection Directive, is largely consistent with that of the e-Commerce Directive. However, a number of points should be noted in this respect. First, the e-Privacy Directive is applicable to passive

Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society and Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

37 Court of Justice, Productores de Música de España (Promusicae) v Telefónica de España SAU, case C275/06, 29 January 2008, para. 70. See also: Court of Justice, Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB, case C461/10, 19 April 2012. See further: S. Kiekegaard, 'ECJ rules on ISP disclosure of subscribers' personal data in civil copyright cases – Productores de Múrica de España (Promusicae) v Telefónica de España SAU (Case C-27/ 06)', Computer Law & Security Report, Vol. 24 No. 3, 2008. C. Kuner, 'Data protection and rights protection on the internet: the Promusicae judgment of the European Court of Justice', European Intellectual Property Review, Vol. 30 No. 5, 2008.

38 See also: Court of Justice, Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB, Case C461/10, 19 April 2012.

39 Article 2 sub a Data Protection Directive.

40 Working Party 29, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.

41 See also: Working Party 29, Privacy on the Internet, WP 37, 21 November 2000.

42 See also: Working Party 29, Opinion 8/2010 on applicable law, WP 179, 16 December 2010.

43 Court of Justice, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, case C73/07, 12 February 2007.

44 This also follows from the interpretation of the concept of 'controller', see inter alia consideration 47 of the Data Protection Directive.

45 Article 2 sub d and e Data Protection Directive.

46 Working Party 29, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010.

Internet intermediaries such as access providers.[47] The directive determines, among other things, that these providers need to adequately secure their networks and that they must process personal data confidentially.[48] Without the consent of the user, for example, providers may in principle not put information on or pull information from a computer device, for example, through the use of a cookie.[49] Further information may in principle only be processed if this is necessary for or related to the provision of the service requested by the user or for related services.[50] With respect to these data processing activities, the providers are responsible for processing these data.

19 Active Internet intermediaries will in principle be considered the controller of data within the context of the Data Protection Directive because they determine the goal and the means of the data processing. This also applies to search engines,[51] as recently evidenced by the Google Spain judgment of the ECJ. In its search engine, Google had referred to a story in a newspaper, that had digitalized its archive and published it online. Mr. Costeja González's name appeared in relation to a real-estate auction connected to proceedings for the recovery of social security debts. The content of the message itself was not illegal, neither was the newspaper requested to remove the announcement from its paper archive or even from its website. The question was whether Google should be obliged to delete the link to the story from its search engine and related to that, whether it could be held responsible for processing personal data because it had indexed the material and made it possible to search the contents of the material. The Court held: "It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing".[52] Consequently, there seems to be a fundamental difference in comparison to the regime under the e-Commerce Directive, because even more active Internet intermediaries can, under certain conditions, invoke the safe harbors therein contained and search engines presumably can too. To recount briefly, the ECJ held in its Google v. Louis Vuitton decision that Article 14 must "be interpreted as meaning that the rule laid down therein applies to an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored."[53]

20 The disparity between the two regimes is aggravated by the fact that the person responsible under the data protection regime is the one who "alone or jointly" determines the purpose and means of the processing. Since active Internet intermediaries typically provide the technical infrastructure and make the platform available, which users use to share their information, they will often be partially or wholly responsible.[54] "Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information. The users of such networks, uploading personal data also of third parties, would qualify as controllers provided that their activities are not subject to the so-called 'household exception'."[55]

21 The active Internet intermediaries will therefore generally be regarded as having a (shared) responsibility for the data processing. There are, however, two important exceptions, namely the household exception and the journalistic exception - the latter is linked to the protection of freedom of expression, as enshrined, among others, in Article 10 ECHR. The first exemption specifies that the provisions of the directive do not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity.[56] In Lindqvist, the ECJ held in this regard that the household exemption in principle does not apply to personal data published on the Internet, even if a site is relatively unknown and used for private purposes only. "That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people."[57] Possibly, the exemption may still apply to webpages

47 Article 3 e-Privacy Directive.

48 Article 4 e-Privacy Directive.

49 Article 5 e-Privacy Directive.

50 Articles 6-9 e-Privacy Directive.

51 See also: Working Party 29, Opinion 1/2008 on data protection issues related to search engines, WP 148, 04 April 2008.

52 Google Spain, para. 33.

53 Court of Justice, Google France SARL, Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA, Luteciel SARL (C-237/08), and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), cases C-236/08, C-237/08 and C-238/08, 23 March 2010, para. 120.

54 See also: Working Party 29, Opinion 5/2009 on online social networking, WP 163, 12 June 2009.

55 Working Party 29, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010, p. 25.

56 Article 3 Data Protection Directive.

57 Court of Justice, Sweden v. Bodil Lindqvist, case C-101/01, 06 November 2003, para. 47.

that can only be accessed with a password or to private profiles on social media that have a limited number of users. The exact boundary between public and private (e.g. in number of users) must be determined on a case-by-case basis. It is important to underline that Internet intermediaries cannot invoke the exception themselves because they are not natural persons.

22 Second, there is an exemption if personal data are processed solely for journalistic purposes.[58] In the Satamedia case, the ECJ stated that this exception does not only apply to media undertakings, but to all those engaged in journalism. The fact that processing is linked to a commercial business model does not mean that it is not an activity solely for journalistic purposes. According to the ECJ, each company after all, engages in undertakings for profit; commercial success may even be the sine qua non for the survival of professional journalism. Furthermore, the means by or the media-type through which the data is transmitted, whether they are conventional carriers such as paper or newer phenomena such as digits, as are used on the Internet, is of no importance. According to the Court, the concept of "journalism'" must be interpreted broadly too, so that non-traditional media companies may also rely on it.[59] This interpretation seems to pave the way for an interpretation under which modern media and active Internet intermediaries using User Generated Content, amateur journalists and bloggers may also invoke the journalistic exception.

23 In the recent Google Spain case, however, a much narrower interpretation was adopted. Although under the interpretation of the ECtHR, Internet intermediaries may also rely on the freedom of expression as protected by the ECHR, the ECJ seems far more hesitant. "Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit [] from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine."[60] It therefore follows that active Internet intermediaries usually have to be considered as the controller of personal data, but in principle cannot invoke the journalistic exception if they are not the editor of the published news story. This constellation, in which the intermediary is a "controller" and in which it cannot invoke an exception, implies that the Internet intermediary must fulfill all obligations under the Directive, such as maintaining transparency, security, confidentiality and the legitimacy of processing personal data.[61]

24 For example, the Internet intermediary needs a legitimate ground for processing personal data. If the information processed concerns data provided by a user about another person (which will often be the case), then the only possible legitimation ground is weighing the interests of the intermediary against the interests of the data subject. This balance will have to be made on a case-by-case basis, but in practice, the fundamental rights and freedoms of the data subject will often prevail.[62] Intermediaries also have to uphold other duties enshrined in the Data Protection Directive, such as the data minimization principle, which specifies that data may only be processed if they are necessary for and proportionate to a clear and specified purpose, that they cannot be further processed for another purpose, that they should be deleted when they are no longer necessary and anonymized when possible.[63] In addition, the directive specifies the right of the data subject to rectification, to have data removed or to oppose, in certain cases, further processing of those data.[64] These duties were initially applied on Internet intermediaries only very cautiously. However, in the case law of the ECJ, a far more extensive interpretation is adopted. Search engines are full-fledged "controllers", according to the court, and consequently they must fulfill all requirements and obligations specified in the Data Protection Directive. Obviously, if this holds true for search engines, there seems to be no reason why this would not also count for (other) active Internet intermediaries.

25 In general, there is a trend towards additional and stronger rights for data subjects and greater and broader obligations for data controllers in data protection law. This appears inter alia from the pending General Data Protection Regulation, which in time will replace the Directive from 1995. It contains numerous new rights such as the right to be forgotten,[65] the right to data portability,[66] which entitles data subjects to transfer their profiles from one to another social network, and the right to resist profiling.[67] The proposed regulation also contains very far-reaching obligations for controllers, such

58 Article 9 Data Protection Directive.

59 Satamedia, paras. 53-62.

60 Google Spain, para. 85.

61 See Articles 16 and 17 Data Protection Directive.

62 Article 7 sub f Data Protection Directive. See also: Google Spain. See further: Working Party 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 09 April 2014.

63 Article 6 Data Protection Directive.

64 Articles 12, 14 and 15 Data Protection Directive.

65 Article 17 General Data Protection Regulation (Commission Proposal).

66 Article 18 General Data Protection Regulation (Commission Proposal).

67 Article 20 General Data Protection Regulation (Commission Proposal).

as the requirement to keep detailed records,[68] to undertake risk assessments[69] and to appoint an internal privacy auditor.[70] Finally, very high penalties are proposed when controllers do not abide by the rules contained in the Regulation, which amount up to 2% of worldwide annual revenue of a company.[71] This can have very serious consequences for the liability and responsibility of active Internet intermediaries. At the time of writing, however, it is still unclear if and when this regulation will be adopted and in what form.

D. Freedom of expression

26 Finally, Internet intermediaries may also rely on fundamental rights themselves. As discussed earlier, many providers do not want to supply personal data of their users to third parties or monitor the communications running through their networks. They may refuse to do so in order to protect the interests of their users, but they may also want to protect their own interests: legal persons may also invoke the right to privacy[72] and data protection to protect their own interests.[73] Alternatively, providers can rely on the freedom of expression, again either directly or indirectly, to protect their own interests or those of their users. Article 10 of the European Convention on Human Rights holds in paragraph 1: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.' Already in the case of Handyside v. UK from 1976, the ECtHR adopted a broad interpretation of this right, linking it to the protection of an open and vital democracy. 'Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man. Subject to paragraph 2 of Article 10, it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'."[74] In later judgments, the ECtHR not only adopted a broad interpretation of the freedom of speech itself, but also of those that may rely on Article 10 ECHR.[75]

27 The fact that Internet intermediaries are one of the parties that may invoke Article 10 ECtHR has recently been confirmed by the ECtHR in the case of Delfi v. Estonia, in which a news site published a critical article about a company that provided ferry services and about L., the sole shareholder. The article itself was nuanced and balanced, the comments of the users posted under the article, however, were less refined. When L. asked the website to remove 20 of these comments and to pay damages, the site removed the comments, but refused to do the latter. In the legal proceedings that followed, the question was posed to which extent the website was responsible for the user comments. A lengthy juridical procedure followed on the national level, in which the website was sometimes treated as an Internet intermediary under the rules of (the implementation of) the e-Commerce Directive and sometimes as a journalistic news medium under the doctrine of freedom of expression, because the site was considered too active to qualify as a passive Internet intermediary. Both in the national proceedings and before the ECtHR, the latter vision ultimately prevailed and the website was treated under Article 10 ECHR and not under the e-Commerce Directive.

28 The argument of the Estonian government before the ECtHR on this point is interesting, as is the rejection of it by the ECtHR: "The Government pointed out that according to the applicant company it had been neither the author nor the discloser of the defamatory comments. The Government noted that if the Court shared that view, the application was incompatible ratione materiae with the provisions of the Convention, as the Convention did not protect the freedom of expression of a person who was neither the author nor the discloser. The applicant company could not claim to be a victim of a violation of the freedom of expression of persons whose comments had been deleted. (...) The Court notes that the applicant company was sued for defamation in respect of comments posted on its Internet portal, it was deemed to be discloser (...)

68 Article 28 General Data Protection Regulation (Commission Proposal).

69 Article 33 General Data Protection Regulation (Commission Proposal).

70 Article 35 General Data Protection Regulation (Commission Proposal).

71 Article 79 General Data Protection Regulation (Commission Proposal).

72 See also: European Court of Human Rights, Colas e.a. v. France, case 37971/97, 16 April 2002.

73 See further: B. van der Sloot, 'Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system', Computer Law & Security Review, 2015-1, p. 26-45. See also the national implementations of the Data Protection Directive, such as that of Austria, and the goals of the e-Privacy Directive.

74 European Court of Human Rights, Handyside v. the United Kingdom, apll.no. 5493/72, 07 December 1976, para 49.

75 See also: http://www.echr.coe.int/Documents/Research_report_Internet_ENG.pdf.

of the comments – along with their authors – and held liable for its failure to prevent the disclosure of or remove on its own initiative the unlawful comments."[76] From this, the ECtHR concluded that the provider was curtailed in its right to freedom of expression. This was confirmed on 16 June 2015 by the Grand Chamber.[77]

29 Consequently, the ECtHR adopts a broad interpretation of the freedom of expression. Parties that remain relatively passive can also invoke Article 10 ECHR, though parties that have no involvement whatsoever, such as purely passive providers, will normally not be able to invoke this right.[78] Some activity or control is necessary; the exact interpretation will depend on the circumstances of the case. In this connection, a comparison can be made with the position of the "controller" under data protection law, although that position primarily entails duties and this one also entails numerous rights and privileges. Although Internet intermediaries, can, under certain conditions, invoke the freedom of expression, this right may be curtailed if the conditions under paragraph 2 of Article 10 of the Convention apply: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

30 It should be noted that Article 8 of the ECHR (right to privacy) is based on Article 12 of the Universal Declaration of Human Rights (UDHR), which states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[79] Although almost all elements of this provision are incorporated in 8 ECHR, the protection of honor and reputation is not. Article 8 ECHR, paragraph 1: "Everyone has the right to respect for his private and family life, his home and his correspondence." The protection of honour and reputation is moved to paragraph 2 of Article 10 ECHR, so that it is not a subjective right which natural persons can invoke, but one based on the grounds on which a state may legitimately curtail the right to freedom of expression.[80] Although the ECtHR has respected this choice of the drafters of the Convention for a long time; since 2007 it has abandoned this line and argued that individuals may, under certain conditions, also invoke a subjective right to the protection of their honor and reputation under Article 8 ECHR.[81] It should also be borne in mind that in general, Article 8 ECHR has been given a very wide scope by the court, which among other things entails that issues surrounding the protection of property and the dissemination of child pornography or similar material (matters that fall under the e-Commerce Directive, rather than the Data Protection Directive in EU law) are also (partially) protected under the right to privacy, under the European Convention on Human Rights of the Council of Europe.[82] Moreover, the right to data protection is also (partially) protected under the scope of Article 8 ECHR.

31 Consequently, in cases like Delfi v. Estonia, two fundamental rights clash. On the one hand the freedom of expression of Internet intermediaries and its users, and on the other hand the right to privacy of third parties. These fundamental rights must be seen as equivalent interests. Consequently, they must be weighed and balanced against each other.[83] "The Court has considered that where the right to freedom of expression is being balanced against the right to respect for private life, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed."[84] Both

76 Delfi v. Estonia (normal chamber), paras. 48 and 50.

77 European Court of Human Rights (Grand Chamber), Delfi/Estonia, appl.no. 64569/09, 16 June 2015.

78 See further: E. Barendt, 'Freedom of Speech', Oxford, Oxford University Press, 2005.

79 See further: UN Documents: A/C.3/SR.119.

80 See in general: http://www.echr.coe.int/library/DIGDOC/Travaux/ECHRTravaux-ART8-CDH(67)5-BIL1338891.pdf.

81 See further: European Court of Human Rights, Chauvy e.a. v. France, appl.no. 64915/01, 29 June 2004. European Court of Human Rights, Pfeifer v. Austria, appl.no. 12556/03, 15 November 2007. European Court of Human Rights, Torres and Polanco v. Spain, appl.no. 34147/06, 21 September 2010. European Court of Human Rights, A. v. Norway, appl.no. 28070/06, 09 April 2009.

82 See among others: European Court of Human Rights, K.U. v. Finland, appl.no. 2872/02, 02 December 2008.

83 European Court of Human Rights, Associes v. France, appl. no. 71111/01, 14 June 2007. European Court of Human Rights, MGN Limited/UK, appl.no. 39401/04, 12 June 2012. European Court of Human Rights, Timciuc/Romania, appl.no. 28999/03, 12 October 2010. European Court of Human Rights, Mosley/UK, appl.no. 48009/08, 10 May 2011.

84 Delfi/Estonia, para. 83. See further: European Court of Human Rights, Springer v. Germany, appl.no. 39954/08, 07 February 2012. European Court of Human Rights, Von Hannover v. Germany (2), appl.nos. 40660/08 and 60641/08, 07 February 2012.

the Chamber and the Grand Chamber of the ECtHR concluded in Delfi v. Estonia that the limitation on the freedom of expression of Delfi by the conviction of the Estonian Supreme Court did not violate Article 10 ECHR.

32 In particular, the ECtHR felt that the measures taken by Delfi were insufficient, i.e. the terms and conditions which prohibited defamatory comments, the notice and takedown system, the monitoring activities and the automatic filter system it employed. Although these measures go beyond what is necessary for the duty of care under Article 14 e-Commerce Directive, they are apparently insufficient when it comes to the duty of care under Article 10 ECHR. A salient detail is that the Court ruled that it was legitimate to hold Delfi liable, while not even trying to press charges against the actual authors of the comments, because Delfi allowed them to post comments anonymously. "It notes that it was the applicant company's choice to allow comments by non-registered users, and that by doing so it must be considered to have assumed a certain responsibility for these comments."[85] This is remarkable because the ECtHR also agrees that the ability to post comments in full anonymity is an important part of both the right to privacy, the right to data protection and the right to freedom of expression; while the efforts to that end by Delfi show that in fact there runs a higher risk of being held liable for the comments of users than if it would not have allowed anonymous comments.

33 Finally, it should be noted that journalists and journalistic media enjoy enhanced protection under the regime of freedom of expression, in part because their role as "public watchdog" is deemed necessary in a democratic society.[86] Journalists also enjoy additional protection of their sources,[87] a larger freedom to engage in newsgathering and a greater protection with respect to publishing classified information,[88] including a limitation of their liability.[89] However, not everyone can invoke the status of journalist; only those who write newsworthy stories and abide by the journalistic principles.[90] With this respect, the ECtHR has chosen to adopt a functional instead of an institutional approach, which means that it does not (only) look at whether a person or company is an established journalist or an established journalistic medium,[91] but rather assesses whether a person or organization contributes to the public debate, engages in journalistic research, observes the journalistic standards, produces newsworthy stories on a more or less regular basis, etc.[92]

34 The European Court of Human Rights has recognized that the Internet-related services of a media enterprise may fall under the scope of Article 10 ECHR: "In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10."[93] To what extent this principle also applies to online platforms, news sites using UGC and amateur bloggers is unclear. Yet it seems that there are no fundamental objections or obstacles for them to rely on these principles. Consequently, sites like Delfi could rely on the journalistic position for the part of their activities that relate to journalism; for example, the story written by one of its employees, which condemned the defamatory user comments and triggered the court case.

35 This line also seems to follow from the recommendation of the Committee of Ministers of the Council of Europe regarding a "New Notion of Media" from 2011,[94] in which it suggests that even amateur bloggers can rely on the extra protection of journalists if they meet the conditions and

85 Delfi/Estland, para. 91.

86 European Court of Human Rights, Barthold/Germany, appl. no. 8734/79, 25 March 1985.

87 See for example: European Court of Human Rights, Financial Times Ltd. e.a. v. United Kingdom, appl.no. 821/03, 15 December 2009. European Court of Human Rights, Ressiot e.a. v. France, appl.nos. 15054/07 and 15066/07, 28 June 2012.

88 See among others: European Court of Human Rights, Stoll v. Switzerland, appl.no. 69698/01, 10 December 2007.

89 See among others: European Court of Human Rights, Fressoz and Roire v. France, appl.no. 29183/95, 21 January 1999.

90 Stoll/Switzerland.

91 European Court of Human Rights, Steel and Morris v. the United Kingdom, appl.no. 68416/01, 15 February 2005. European Court of Human Rights, Társaság a Szabadságjogokér v. Hungary, appl.no. 37374/05, 14 April 2009.

92 See also: http://www.ivir.nl/publications/helberger/Making_User_Created_News_Work.pdf.

93 European Court of Human Rights, Times Newspaper LTD(1 and 2)/UK. See also: European Court of Human Rights, Mosely v. UK. Again, this seems to create a tension between the approach of the ECtHR and that of the ECJ in its Google Spain decision, namely in connection to the use and protection of archives and archival functions. See also the case Wegrynowski and Smolczewski v. Poland, in which the ECtHR explicitly stated: 'The Court accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations. Furthermore, it is relevant for the assessment of the case that the legitimate interest of the public in access to the public Internet archives of the press is protected under Article 10 of the Convention.' European Court of Human Rights, Wegrynowski and Smolczewski/Poland, appl.no 33846/07, 16 July 2013, para. 65.

94 Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media.

journalistic standards. "As regards in particular new media, codes of conduct or ethical standards for bloggers have already been accepted by at least part of the online journalism community. Nonetheless, bloggers should only be considered media if they fulfil the criteria to a sufficient degree."[95] It should be noted that in order to rely on the regime for journalists under the freedom of expression, actors should abide by a number of additional duties of care and principles. Consequently, if Internet intermediaries want to rely on this position, they should abandon their traditional passivity even further.

E. Conclusion

36 The e-Commerce Directive was adopted at the beginning of this millennium to harmonize the various national approaches to the liability of Internet intermediaries for wrongful acts conducted by their users through their networks. The fear was that the existing diversity at that time would lead to legal inequality and uncertainty, which could hamper the digital economy. It was decided to exclude passive Internet intermediaries, under certain conditions, from liability for actions conducted by their users. Although this regime is still ensured for these traditional Internet providers, a number of factors have complicated this system.[96]

37 First, providers have become increasingly active, for example by indexing information and making it searchable, by creating social platforms and by creating sites which are based on User Generated Content. The question is whether they can also rely on the safe harbors for liability specified in the e-Commerce Directive. The ECJ seems to allow active Internet intermediaries to invoke these safe harbors to a relatively large extent, on the condition that these providers assume additional duties of care. This may create a Catch-22 situation. Providers that are more active have more control over the content they distribute and are thus supposed to have greater duties of care, but these duties of care imply that the Internet intermediaries gain even further control over the content. This might mean that they must adopt even further standards of care and exercise even greater control.

38 Secondly, the e-Commerce regime does not apply to issues falling under the data protection regime. For passive Internet intermediaries, the two regimes are more or less comparable. Under the Data Protection Directive, passive actors are in principle exempt from responsibilities and duties of care. For active intermediaries, however, the data protection regime is substantially different from the e-Commerce regime. The Data Protection Directive imposes many duties on active Internet intermediaries and this burden will only be intensified when the General Data Protection Regulation is adopted. Active Internet intermediaries can rely on the exclusion of liability under the e-Commerce regime much more quickly than under the data protection regime.

39 Thirdly, Internet intermediaries increasingly rely on fundamental rights themselves, to protect their own interests or those of their users. One example that has not even been discussed in this paper is the freedom to conduct a business, as enshrined in Article 16 of the EU Charter of Fundamental Rights. What has been discussed is that Internet intermediaries may rely on data protection law to protect their own data or those of its users. Internet intermediaries are sometimes asked to provide information about users (that are suspected to have carried out unlawful activities via their networks) to third party right holders (often of intellectual property), to monitor their networks and to detect or block infringing activities. Internet intermediaries often find themselves in a difficult position, having to judge the legitimacy of the claims and having to balance the rights of two different parties. As in Europe, in contrast to the DMCA in America, no legislative framework exists for the handling of such requests and these decisions are often made before a case is judged by a court of law; thus, Internet providers often have to make an assessment of the case independently and assume the role of a judge.

40 Providers additionally rely on the freedom of expression. This may be an indirect claim in order to protect the freedom of expression of users of a platform against filter obligations or against obligations to remove certain messages, information or files. More importantly, providers can also rely on the freedom of expression themselves, for the protection of their own interests, even if they are considered responsible for illegitimate actions of the users of their services through their network. This predominantly applies to active Internet intermediaries, as purely passive providers that provide storage space for third parties and mere conduits will usually not qualify as a publisher or an initiating party in the publication, distribution or gathering of information. If an active Internet intermediary successfully invokes the freedom of expression, then it is this right that should be balanced and weighed against the rights of the third party, such as his copyright. To further complicate matters, what has remained undiscussed in this

95 CM/Rec(2011)7, nr. 41-42.

96 See further: T. Synodinou, "Intermediaries' liability for online copyright infringement in the EU: evolutions and confusions',Computer Law & Security Review, Vol. 31 No. 1, 2015. P. van Eecke, 'Online service providers and liability: a plea for a balanced approach', Common Market Law Review, Vol. 48 No. 5, 2011.

contribution are third parties' rights to freedom of expression or the freedom of enterprise, for which being findable in search engines like Google may be pivotal. Moreover, third parties' claims may also revolve around privacy and data protection interests. This can also be invoked against the freedom of expression of the provider.

41 It should be stressed that in most freedom of expression regimes around the globe, a special position is reserved for journalists. Traditionally, they have more rights, wider freedoms and enjoy greater protection from liability. It seems that there are no obstacles for Internet intermediaries such as news sites that use UGC to claim such a position as well, provided that they comply with the additional safeguards and obligations that go with being a journalist. It should be remembered that in order to obtain the "status" of a journalist, the provider's passivity is put under pressure to an even greater extent. Consequently, there is a certain tension between the different regimes. The most striking consequence is perhaps that providers are encouraged to either remain fully passive (and therefore have no form of control over their services), in order to qualify for the exemption from liability under the e-Commerce and the data protection regime, or to abandon their passivity almost fully (and gain a very large form of control over the actions of their users), in order to rely on the freedom of speech and possibly even to qualify for the position of a journalistic medium.[97]

42 It follows that Internet intermediaries can rely on a variety of different positions and regimes. Each of the three regimes discussed here (the e-Commerce Directive, the Data Protection Directive and the freedom of expression contained in the ECHR) has roughly three positions.

43 Under the e-Commerce Directive:

- (1) The passive provider is normally excluded from liability if it complies with the requirements specified in the Directive.
- (2) Active providers that adopt additional measures and safeguards can also rely on the exclusion of liability.
- (3) There are providers that are so active that they simply do not qualify as an Internet intermediary; for example publishers of news-sites with respect to the stories written by their own employees and posted on their own website.

44 Under the Data Protection Directive:

- (1) The data processor who acts under the authority of the data controller has to take into account the limited safeguards specified in the e-Privacy Directive only.
- (2) Active Internet intermediaries that, for example, determine the technical infrastructure (and thus the means of processing) of a website, but depend primarily on the users of the site for the content and the material, have a shared responsibility with the users.
- (3) The Internet intermediaries that are so active that they are solely responsible for the data processing must comply with all the obligations contained in the Data Protection Directive, and in the future the General Data Protection Regulation.

45 Under the doctrine of freedom of expression:

- (1) Providers that are so passive that they cannot rely on this regime because they do not share, gather or publish any information themselves.
- (2) Active Internet intermediaries that can invoke the freedom of expression.
- (3) Providers who comply with additional safeguards and obligations may rely on the privileged status of journalist.

46 Not only does each position entail different rights and obligations, but different conditions apply to the positions as well. For example, the freedom of expression of a provider may be limited, even if it has taken measures that would be sufficient in relation to the intensified duty of care for active providers under the e-Commerce Directive. Moreover, providers will more quickly be able to rely on the exclusion of liability under the e-Commerce Directive, possibly by fulfilling additional duties of care, than to invoke the position of processor under the Data Protection Directive. Active providers have many duties and obligations under the Data Protection Directive, while they have many freedoms and privileges under the freedom of expression. It should also be noted that the regimes of the European Union, including that of the e-Commerce Directive and the Data Protection Directive, and the instruments of the Council of Europe, including the ECHR, deviate on a number of points. This is reinforced by Article 8 ECHR, which also provides partial protection to private property and against criminal acts, while these matters are treated under the e-Commerce Directive rather than the Data Protection Directive

97 See also: G. González Fuster, 'Balancing intellectual property against data protection: a new right's wavering weight', IDP: Revista de Internet, Derecho y Política, No. 14, 2012. M. Husovec, 'Injunctions against innocent third parties: case of website blocking', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 4 No. 2, 2013.

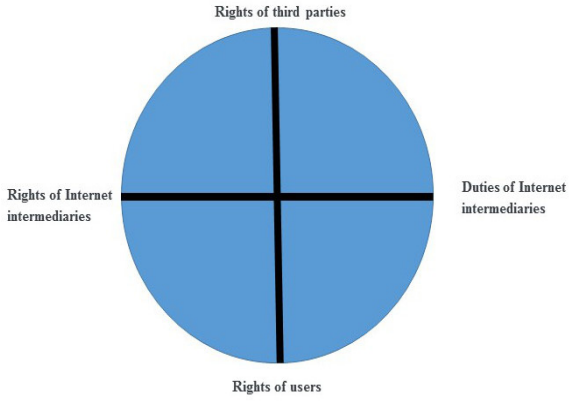
in EU law. Article 8 ECHR also covers rules on data protection, but this right is treated and explained in substantially different terms by the ECtHR than by the ECJ.[98]

47 In conclusion, while the e-Commerce Directive was installed to clarify the position of and to provide greater legal certainty to providers (given the great diversity in national rules that existed before the entry into force of the Directive), it should be acknowledged that the current situation in Europe regarding the liability of Internet intermediaries is still very diffuse and unclear. Consequently, despite the rules contained in the Directive, countries in Europe have a very different take on many of the complex questions and positions. Courts and judges will often have a very wide margin of appreciation and thus a responsibility for weighing and balancing the different interests and positions involved, while there are usually very few cases that make it to the national supreme courts, let alone the European courts. Most cases are dealt with by lower courts and the case law is often contradictory. Additionally, Internet intermediaries themselves have an important role regarding balancing the various interests and circumstances of the case and this creates an even more diffuse picture, because of the different attitudes and approaches by the various providers.[99]

48 The solution should therefore be twofold. First, a system could be implemented in which not the Internet intermediary, but a court will assess requests from third parties. This would ensure that it is not the Internet intermediary that is primarily responsible for the initial evaluation of the case, but a judge. This would simply require a rule specifying that all requests from third party rights holders should be judged by a court of law. Secondly, judges would be helped by a simplification of the rules and a harmonization of the different regimes. This requires installing one regime for determining the liability of Internet providers in Europe. Moreover, there should be clarity about the parameters that judges must take into account when establishing the liability of Internet intermediaries. Such a system would need to be adequately clear to avoid legal uncertainty, but should also allow for sufficient flexibility in order to effectively respond to new technological developments.

49 One option would be to opt for a system that does not depend on fixed positions of Internet intermediaries, with corresponding duties and freedoms, but on a more graduated approach. Specifying the exact details of such a system lies beyond the scope of this article, but with some simplification, two axes could be distinguished. The first axis contains the rights of the user in relation to the rights of third parties - they should always be balanced and weighed against each other. If a third party submits a poorly substantiated claim or provides only marginal evidence, the user's interests will usually prevail. If, however, the behavior of the user is clearly illegal and substantially harms the interests of third parties, the opposite would hold true. The second axis concerns the rights and freedoms of the Internet intermediary on the one hand and its duties and responsibilities on the other. These two sides must also be weighed and balanced by a court. Perhaps it would be advisable to choose a form of sectoral co-regulation, such as Article 27 of the Data Protection Directive, which explicitly encourages codes of conduct. For now, however, the liability regime for Internet intermediaries in Europe remains a jumble of different positions, regimes, rights, duties and exemptions. It is to be expected that for the time being, no substantial changes will be made. Welcome to the world of Internet liability, welcome to the jungle.

50 The liability of Internet intermediaries:



51 Some questions remain to be answered regarding this approach however, such as who should develop the concrete rules, what are the limits thereof, who should create or clarify the framework that judges should endeavour to apply, should they do it themselves, etc.? As mentioned, the American Digital Millennium Copyright Act might provide some leads for this alternative approach. For this reason, a brief description of this Act is given below. The DMCA specifies that a service provider shall not be liable for monetary relief, or for injunctive or other equitable

98 P. de Hert & S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in: S. Gutwirth, Y. Poullet, P. de Hert, J. Nouwt en C. De Terwangne (eds), 'Reinventing data protection?', Dordrecht, Springer Science, 2009.

99 See further: S. de Vries, 'Balancing fundamental rights with economic freedoms according to the European Court of Justice', Utrecht Law Review, Vol. 9 No. 1, 2013. L. Edwards, 'The fall and rise of intermediary liability online' In: L. Edwards, L. and C. Waelde (eds.), Law and the Internet, Hart Publishing, Oxford, 2009.

relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider does not have actual knowledge that the material or an activity using the material on the system or network is infringing, in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent, or upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material. A further condition is that the provider does not receive a financial benefit directly attributable to the infringing activity, in the case in which the service provider has the right and ability to control such activity. A final condition is that upon notification of claimed infringement, the provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity. This resembles the e-Commerce regime to a large extent.[100]

52 However, the rules regarding the notice and takedown regime are specified in further detail.[101] The DMCA specifies that the service provider should have a designated agent to receive notifications of claimed infringement, by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, the name, address, phone number, and electronic mail address of the agent and other contact information which the Register of Copyrights may deem appropriate. The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.[102]

53 The DMCA continues by specifying the elements of the notification. A notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes, first, a physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. Second, identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. Third, identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. Fourth, information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complainant may be contacted. Fifth, a statement that the complaining party has a good reason to believe that use of the material under scrutiny is not authorized by the copyright owner, its agent, or the law. Sixth and finally, a statement that the information in the notification is accurate, and under penalty of perjury, that the complainant is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.103

54 The DMCA explicitly states that if the copyright owner fails to comply with these provisions, the notification to the provider shall not be considered in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent. If there are minor flaws in the notification, this rule only applies if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions and requirements. Furthermore, the DMCA contains an explicit clause on misrepresentation. It holds that any person who knowingly materially misrepresents that material or activity is infringing,

100 See for comparison with EU regulation: M. Peguera, "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems." Columbia Journal of Law & the Arts 32, 481, 2009. V. McEvedy, "The DMCA and the Ecommerce Directive." EIPR 24.2, 2002.

101 In the USA, the Communications Decency Act is also of relevance: J. Band and M. Schruers, 'Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act', Cardozo Arts & Ent. LJ 20, 295, 2002.

102 See for comments on specific cases: M. Driscoll, 'Will YouTube Sail into the DMCA's Safe Harbor or Sink for Internet Piracy', J. Marshall Rev. Intell. Prop. L. 6, 2006. T. A. Dutcher, 'Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in RIAA v. Verizon Internet Services', Santa Clara Computer & High Tech. LJ 21, 493, 2004. A. Kao, 'RIAA v. Verizon: Applying the Subpoena Provision of the DMCA', Berkeley Tech. LJ 19, 405, 2004. E. C. Kim, 'YouTube: Testing the safe harbors of digital copyright law', S. Cal. Interdisc. LJ 17,139, 2007. B. White, 'Viacom v. YouTube: A Proving Ground for DMCA Safe Harbors Against Secondary Liability', John's J. Legal Comment, 24, 811, 2009.

103 See for an explanation and further discussion: L. Chang, 'Red Flag Test for Apparent Knowledge under the DMCA Sec. 512 (C) Safe Harbor', Cardozo Arts & Ent. LJ 28, 195, 2010. E. Lee, 'Decoding the DMCA safe harbors', Columbia Journal of Law & the Arts, Forthcoming, 2009. Mark A. Lemley, Mark, 'Rationalizing Internet Safe Harbors', Journal of Telecommunications and High Technology Law 6, 101, 2007. C. E. Mammen, 'File Sharing is Dead-Long Live File Sharing-Recent Developments in the Law of Secondary Liability for Copyright Infringement', Hastings Comm. & Ent. LJ 33, 443, 2010. J. M. Miller, 'Fair Use through the Lenz of Section 512 (c) of the DMCA: A Preemptive Defense to a Premature Remedy', Iowa L. Rev. 95, 1697, 2009. M. Piatek, T. Kohno and A. Krishnamurthy, 'Challenges and directions for monitoring P2P file sharing networks, or, why my printer received a DMCA takedown notice', HotSec, 2008.

or that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is ill-treated by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

55 The Act also provides rules on the replacement of removed material.[104] The DMCA specifies that a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing. This rule, however, shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice, unless the service provider, first, takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material. second, upon receipt of a counter notification, promptly provides the person who provided the notification with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and third, replaces the removed material and ceases disabling access to it not less than 10, nor more than 14 business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.[105]

56 Finally, the DMCA specifies the contents of counter notification. A counter notification must be a written communication administered to the service provider's designated agent that includes, first, a physical or electronic signature of the subscriber; second, identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled; third, a statement under penalty of perjury that the subscriber has a good reason to believe that the material was removed or disabled due to a mistake or misidentification of the material to be removed or disabled; fourth and finally, the subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification or an agent of such person.[106]

57 Thus, the advantage of the DMCA over the e-Commerce Directive is that it specifies in further detail what the obligations and rights of the different parties are. The Act describes who should issue the notification on a copyright infringement, to whom, and what information the notification should contain. Importantly, it states that if the notification is not issued in a correct manner, it shall not be considered when establishing the question of whether the Internet intermediary had knowledge of the copyright infringement. Therefore, the burden is placed on the copyright owner, not on the Internet intermediary. More importantly, the DMCA explicitly lays down sanctions for those that purposely misrepresent the truth. Thus, if a person misrepresents himself as a copyright owner or if a copyright owner notifies an Internet intermediary that his copyright has been infringed while he knows or should know that this is not the case, the costs are for that person to bear, not for the Internet intermediary. Furthermore, the third party (usually the user of the Internet provider's service) has an explicitly recognized role in the DMCA. It can issue a counter notification and argue that its use of the alleged infringing material is actually legitimate. Again, the Act specifies in detail how the counter

104 However, there is also critique on the working of the DMCA: W. Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment', Harv. JL & Tech. 24, 171, 2010. J. Bretan, 'Harboring Doubts about the Efficacy of 512 Immunity under the DMCA', Berkeley Tech. LJ 18, 43, 2003. J. Cobia, 'Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process', Minn. JL Sci. & Tech. 10, 387, 2008. G. Jansen, 'Whose Burden Is It Anyway: Addressing the Needs of Content Owners in DMCA Safe Harbors', Fed. Comm. LJ 62,153, 2010.

105 See in further detail: D. Weinstein, 'Defining Expeditious: Uncharted Territory of the DMCA Safe Harbor Provision-A Survey of What We Know and Do Not Know about the Expeditiousness of Service Provider Responses to Takedown Notifications', Cardozo Arts & Ent. LJ 26, 589, 2008.

106 See for an application of the DMCA on new developments: B. Brown, 'Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World', Berkeley Tech. LJ 23, 437, 2008. J. J. Darrow and G. Ferrera, 'Social networking web sites and the DMCA: a safe-harbor from copyright infringement liability or the perfect storm?', Northwestern Journal of Technology & Intellectual Property 6.1, 2007. M. S. Sawyer, 'Filters, fair use & feedback: user-generated content principles and the DMCA', Berkeley Tech. LJ 24, 363, 2009. C. W. Walker, 'Application of the DMCA safe harbor provisions to search engines', Va. JL & Tech, 9, 1, 2004.

notification should be issued. The DMCA gives a clear time path for the Internet provider, when to remove the content, when to notify the user of the copyright infringement notification, when to notify the copyright owner of a counter notification, when the content should be restored, and when the matter must be resolved by a judge. Consequently, if the Internet provider follows the clear and detailed instructions and the time path, it runs no risk of being held liable for any damages - either at the side of the copyright owner or at the side of the user.

58 There is no reason why this model should not be applied to privacy infringements in Europe as well. It would help to shed a light on the dark jungle that is the Internet intermediary liability regime in Europe right now. One addition would be important, namely that the Internet provider is at liberty to overrule either the complainant's or the defendant's claim or counter-claim on its own initiative to protect its own direct or indirect interests. This of course would be at its own discretion. If a provider would overrule a notification or counter-notification on its own initiative for no apparent reason, then it would be liable for the damages following from that action. If it did so mistakenly, but in good faith, a judge might overrule him in a legal procedure. Consequently, both the claimant and the defendant would also have the right to go to a court in case an Internet provider overrules their notification or counter-notification.

59 So let's suppose the situation in which a news portal is partly based on User Generated Content and partly on content produced by employees. The portal publishes a news item, written by one of its employees on a politician that might have been paid by a company to vote against a certain Bill. The site allows users to change or elaborate on the story; one user does and reveals that the politician had an extra-marital affair with the daughter of the CEO of the same company, making him vulnerable for blackmail. He does not cite a public source, but confidentially reveals to the Internet provider that he has contact with the daughter of the CEO and heard the story from her first hand. The Internet provider is not in any position to check this claim. The politician decides to complain to the news portal and to request the removal of the unsupported claim that he has or had an extramarital affair and has been or could have been blackmailed. It is up to the Internet provider to make a decision.

60 Under the current regime, the Internet provider is under a twofold burden. On the one hand, it has the leading role in establishing the facts and the actions taken thereupon. First, it has to assess the reliability and the veracity of the complaint by the politician. Second, it has to assess the reliability of the story of the user. Third, even if it is true, it has to balance the infringement of the politician's privacy against the public interest in knowing the facts disclosed. Fourth, there is no or only limited room for the Internet provider to take into account its own interests (either in being a trustful website not making false or unsubstantiated claims or in being a leading website bringing breaking news and scoops) and those of its readers. On the other hand, it might even be sued by either the politician or the user if it makes a wrongful decision and a judge might, as evidenced by Delfi v. Estonia, be held to pay a fine or damages. A judge might impose even further obligations on the provider, without being clear on how the obligations should be implemented or weighed with the other interests at stake.

61 The alternative approach would ameliorate this situation in two ways. On the one hand, it gives a clear indication regarding what information the notification by the politician should contain, that the provider should take down the alleged infringing information and that it should notify the user of the takedown. If the user subsequently argues that the story was indeed true and legitimate, the provider has to inform the politician thereof and restore the content. If the parties still disagree, the matter shall be resolved by a court of law. If the Internet provider follows this procedure, it cannot be held liable for damages either by the politician or by the user. In addition, this system has the benefit as it allows the Internet intermediary to take into account its own direct or indirect interests. For example, even though the user might claim that he is sure that the story is true and legitimate, the provider still runs the risk that a judge will rule otherwise. This would presumably not be a problem for a gossip magazine, but for a quality news portal this might be problematic because it undermines the name of the newspaper. Similarly, a quality news portal could, for example, have the policy of only publishing stories on the public lives of public figures, not about their private lives and so decide to reject the story by the user to protect the integrity and corporate identity. This decision could be challenged by the user, for example arguing that the private life of the politician had an effect on his profession.

62 On the other hand, the judge would have a clearer decision tree to arrive at his or her conclusion. Of course, the judge has to determine the truthfulness of the story. Presuming the court would hold the story to be true, it would then not only balance the freedom of speech of the user against the right to privacy/reputation of the politician, but also the interests of the Internet intermediary and of its users. Moreover, it would take into account the steps taken by the Internet provider to prevent or minimize damage to the politician, for example, by letting an employee verify the story written by the user. The court would then consider all these values and interests and weigh and balance them against

each other. This would not only make it easier for the court to arrive at its decision, it would also become clearer for the parties involved how the court arrived at its decision, which interests were taken into account and how they were balanced and weighed against each other.

* Bart van der Sloot is a researcher at the Institute for Information Law, University of Amsterdam, the Netherlands. This article contains revised and updated parts of an article that has appeared in Dutch. B. van der Sloot, 'Welcome to the jungle: de aansprakelijkheid van internet-intermediairs voor privacyschendingen in Europa', SEW - Tijdschrift voor Europees en economisch recht, 2014-10.