Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web

Mario Viola de Azevedo Cunha*, Luisa Marin**, and Giovanni Sartor***

Abstract

- Since the adoption of the EU e-Commerce Directive, web hosting has dramatically changed. User-generated content is usually uploaded onto platforms that facilitate and support users in preparing content and making it available. Commercial companies who make a profit by associating advertisements to user-generated materials run such platforms in most cases.
- We shall address the legal framework applicable to ISPs managing platforms for user-generated contents. Can they be viewed as mere host providers, even though their activities include not only distributing content, but also indexing it and linking it to advertisements?
- As user-generated-content often concerns third parties, we shall consider whether liability exemptions for ISPs are applicable to data protection violations regarding third parties' information uploaded by users.
- We shall address this issue through a comparative analysis of cases, taking into account decisions of the European Court of Justice (ECJ) and of the European Court of Human Rights (ECtHR), the case law of some EU member states (in particular France and the Netherlands), as well as opinions of national data protection authorities.

Introduction: user-generated content and the privacy of third parties

In the era of the so-called web 2.0 most content available online is user-generated: many (and potentially all) users of the Internet participate in re-writing the web's hypertext, and they mostly do that by interacting with other individuals in unprecedented forms of collaboration. As Tapscott and Williams[1] put it:

> We're all participating in the rise of a global, ubiquitous platform for computation and collaboration that is reshaping nearly every aspect of human affairs. While the old Web was about Web sites, clicks, and 'eyeballs', the new Web is about the communities, participation and peering. As users and computing power multiply, and easy-to-use tools proliferate, the Internet is evolving into a global, living, networked computer that anyone can program.

'Programming' here needs to be understood in the broadest sense, including any way of 'writing' the web: uploading textual or multimedia content in online repositories, creating one's personal blog and linking it to other blogs or pages, creating one's image and establishing connections with one's fellows in a social network, participating in collaborative enterprises aimed at producing software or works of authorship.

In the context of the web 2.0 the relationship between providers of web hosting and addressees of such a service has significantly changed. In 2000, when the EU e-Commerce Directive was passed,[2] web hosting consisted mainly in websites (html pages and related documents) completely developed by the recipient of

* State Attorney of the Municipality of Saquarema (Brazil) and holds a PhD in Law from the European University Institute (Italy) and an LLM in Private Law from Rio de Janeiro State University (Brazil). Email: Mario.Cunha@EUI.eu.

** Assistant Professor in European Law at the University of Twente (The Netherlands). Email: l.marin@utwente.nl.

*** Professor of Legal Informatics and Legal Theory at the European University Institute (Italy) and Professor of Computers and Law at the University of Bologna (Italy). Email: giovanni.sartor@gmail.com.

1 Don Tapscott and Anthony D Williams, *Wikinomics: How Mass Collaboration Changes Everything* (Portfolio, 2008) 19.

2 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), [2000] OJ L178/1.

the hosting service, including the way the content was posted, the structure of the websites and so on. The host provider only made available the server (disk-space and processor) for storing the website, the connection from that server to the Internet, and the software (the web-server) that would provide access to the website (by typing a domain name or using a search engine). While the recipient of the service had the greatest freedom in developing the website according to his or her tastes and preferences, editing web pages was relatively difficult and complicated, and thus the web could not be a creative space for the majority of people.[3]

Web hosting has dramatically changed in the last years. Now platforms are available that facilitate the creation and distribution of online contents, thus enabling everyone to participate in these activities. Among the most popular platforms used worldwide we can name iTunes and YouTube for videos, Facebook for personal information, Wordpress for blogs, Twitter for short messages, e-Bay for auctions; the list is far from being exhaustive. Such platforms, to a different degree, support the creative activity of the users: first, they provide facilities (and constraints) for creating content, such as page templates, ways to organize the information and link it, apps for an infinite variety of functions; secondly, they facilitate the retrieval of the user-generated materials, by indexing, classifying, ranking them (usually by aggregating users' preferences and choices). Such platforms are mostly run by commercial companies that usually make a profit by associating advertisements to the user-generated materials, often by selecting the ads on the basis of the content of such materials. Google, whose mission is 'to organize the world's information and make it universally accessible and useful',[4] exemplifies this business model.

The web 2.0 represents an evolution whose scope goes beyond computing and the Internet, to reach the whole system of media, information, and communication. It is not by chance that Internet freedom is considered nowadays among the parameters to measure the level of democracy of a state;[5] and that the new media (from mobile phones to social networks) have arguably played the role of catalyst in the recent political changes in the North African states.[6] Thus, in the framework of the web 2.0, the web has become a forum where everyone can effectively exercise their civil, economical, and political rights. It is also the place where one can develop one's social personality, present oneself to others, and engage in social relationships. This beneficial function of the web, as a fundamental enabler of individual and social development, is supported by the activity of profit-seeking private companies, whose service provides the precondition for the exercise of such rights, and pre-determine to some extent the ways in which they are exercised.

Unfortunately, the production and distribution of user-generated content is not always socially beneficial: consider for instance defamation, violation of intellectual property, support of criminal activity, incitement to hate, child pornography, etc. This has raised a number of legal issues that have been extensively discussed in the literature in recent years.[7] Here we shall mostly focus on one legally problematic aspect of user-generated content, namely, the inclusion of personal data concerning third parties.

We must point out that web-based platforms are mostly used by people to distribute their own personal information, and to tell others about themselves, for a variety of different purposes. The publication of self-related content may consist just in expressing one's own attitudes, tastes, preferences, capacities; it may be directed at advertising oneself, for the purpose of getting access to economic or social opportunities; or it may even be part of one's professional activity, which

3 Giovanni Sartor and Mario Viola de Azevedo Cunha, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (2010) 18(4) International Journal of Law and Information Technology 15.

4 Google's mission statement from the outset. From Wikipedia, available at <http://en.wikipedia.org/wiki/Google> accessed 26 April 2011.

5 See, for instance, United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of the United Nations, available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf> accessed 26 July 2011, 4: 'Indeed, the recent wave of demonstrations in countries across the Middle East and North African region has shown the key role that the Internet can play in mobilizing the population to call for justice, equality, accountability and better respect for human rights. As such, facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.'

6 We refer to Egypt's protests in 2011, which have been defined in the blogosphere as 'a social media revolution', at <http://diversity.prsa.org/index.php/2011/02/ a-social-media-revolution-the-egypt-protests-and-the-role-of-new-media/> accessed 14 April 2011. See also <http://www.blogworld.com/2011/01/28/social-medias-role-in-the-egyptian-protests/> accessed 14 April 2011.

7 See, for instance, Lesli C Esposito, 'Regulating the Internet: The New Battle Against Child Pornography' (1998) 30 Case Western Reserve Journal of International Law 541; Sewali K Patel, 'Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go' (2002) 55 Vanderbilt Law Review 647; Todd M Hinnen, 'The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet' (2004) Columbia Science and Technology Law Review; Catherine Fancher and G Harvey Dun III, 'The Trend toward Limited Internet Service Provider (ISP) Liability for Third Party Copyright Infringement on the Internet: A United States and Global Perspective' (2002) Business Law International 143.

may include informing the public about one's skills, interests, published work, previous work relations, etc. This use of the Internet appears to be incompatible with some paternalistic data protection rules, literally understood. Consider for instance the provision contained in various EU member states' data protection regulations according to which sensitive data can be published only with the authorization of the data protection authority.[8] Assume that a gay person decides to 'come out of the closet', and to declare his sexual identity in his blog or public Facebook profile. It would appear that he has published sensitive private data with the consent of the data subject (himself), but without the authorization of the data protection authority, committing therefore a punishable offence. The provider would have committed the same offence, if the latter were considered responsible for data protection offences committed by using its platform. The same would apply to a person affected by breast cancer, who tells on her online blog how she is bravely fighting against her illness, without losing hope and interest in life, to encourage others to do the same. She would be engaging in an illicit activity, for publishing health information without the required authorization.

While it seems absurd to restrict, through data protection rules, self-presentations on the web (no sensible judge, we think, would endorse the literal application of such regulations), the problem is much more complex when data concerning others are published online. In fact, the online distribution of user-generated content including third parties' personal data can involve a violation of data protection rights, since it may take place outside of the conditions established by data protection law (in particular, without the consent of the concerned individual). This violation is aggravated by the fact that once data have been distributed over the Internet, they circulate in innumerable copies, over which the data subjects do not have a real possibility to exercise control.

However, the publication of materials containing the personal data of third parties may also pertain to the exercise of fundamental civil and political rights. Consider for instance the case when a person uploads third parties' information having public relevance (eg concerning the activity of individuals having a significant political or economic role, or a significant social visibility). This may well fall within freedom of expression and even of the press (by broadly understanding as 'press' any 'publication which affords a vehicle of information and opinion'[9]). Or, consider the case when one publishes information about oneself that also concerns others, such as (more or less artistic) pictures of oneself with others, or diary pages pertaining to one's life encounters.[10] Another example concerns online stories which give clues linking the fictional narration to particular individuals (here the freedom of communication or artistic expression would be at issue).

All such cases involve what we consider to be peer violations of privacy interests, namely impingements on individuals' data protection rights by other, similarly located, individuals. Such violations deserve specific analysis since they are very different from the prototypical interferences in privacy and data protection, as we knew and conceptualized them before the advent of the user-generated web. While the latter violations usually involve the disproportionate relationship between an individual and a big organization, a public or private 'big brother', peer violations concern the equal interactions between private persons; rather than the clash between individual rights and corporate or public interests we have the clash between conflicting individual rights (privacy versus freedom of expression, freedom of association, or freedom to develop and express one's personality).

In the following pages we shall consider how providers' liability for peer violations of data protection has been addressed in the case law of different countries. In particular we will consider whether liability exemptions for providers are applicable to violations regarding third parties' information uploaded by users; and, if so, under which circumstances such exemptions are limited. First, the European legal framework for data protection will be presented, and in particular the exemptions from liability contained in the e-Commerce Directive, in connection with the principle of neutrality. Then we will analyse the judicial experience of cases involving ISP liability for user-generated content, giving special attention to issues related to data protection. We will take into account the decisions of the European Court of Justice (ECJ) and the European Court of Human Rights (ECtHR), national decisions (in particular from France and the Netherlands), as well as opinions of the national data protection authorities. Finally, we will conclude with some observations and proposals.

8 This is the case, for example, under Italian data protection law, referred to below in the section discussing the other EU member states, Italy and Spain.

9 Yochai Benkler, 'A free irresponsible press' (2011) 46 Harvard Civil Rights-Civil Liberties Law Review 359.

10 See for instance, Daniel Solove, *The Future of Reputation* (Yale University Press, 2008).

The personal data of third parties—between privacy and freedom of expression: the European legal framework

While in the USA privacy issues related to the processing of personal data in the private sector are largely dealt with by a self-regulatory, market-based approach,[11] in Europe personal information is a matter of fundamental rights, EU directives, and ordinary legislation. The protection of personal data has a high priority in the EU legal and policy agenda, and now enjoys constitutional status. In fact, the Lisbon Treaty provides the legal basis for the accession of the EU to the European Convention on Human Rights (ECvHR) and gives binding effects to the EU's Charter of Fundamental Rights, two instruments providing for the protection of privacy and data protection.[12] The first instrument addresses privacy through its Article 8, devoted to the respect of one's private and family life, home and correspondence, whereas the second one contains a specific provision for data protection (Article 8, which states that 'everyone has the right to the protection of personal data concerning him or her').

The EU Charter spells out of the essential aspects of the EU model for data protection: due process, the principle of consent, and the rights of access and rectification.[13] The scope of personal data in the EU, however, differs from one member state to the other, since national legislators have exercised a certain degree of discretion in implementing the EU instruments on data protection. For instance, Portugal considers information concerning deceased people as personal data, while the UK does not.[14] The diversity of national approaches to this issue is constrained by the case law of the ECJ, which, for instance, has recently ruled that IP addresses 'are protected personal data because they allow those users to be precisely identified.'[15]

Most of the principles of the Charter of Fundamental Rights constitutionalize the pre-existing legislative framework, whose main instrument is the EU Data Protection Directive (hereinafter DPD).[16] This legislative framework has the aim of protecting the rights of the data subjects, while contributing to the proper functioning of the internal market by ensuring the free movement of information society services and of personal data between the member states. It establishes a series of duties and rights for all stakeholders and constrains the processing of personal data through binding rules, while providing some exceptions to these rules for the sake of other values, such as freedom of expression and literary and artistic expression.

According to the DPD, legitimate processing of personal data must have a legal basis. In particular, the consent of the data subject is often required when personal data are processed by private entities (except when data are needed for managing contractual relationships). For sensitive data, consent has to be expressed, and many EU member states also require an authorization by the national data protection authority.[17]

There are however, various limitations to data protection, for the sake of a number of important legal values. First of all, Recital 17 of the DPD states that 'as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned . . . the principles of the Directive are to apply in a restricted manner.' Recital 37 goes in the same direction, by recognizing that 'the processing of personal data for purposes of journalism or for purposes of literary or artistic expression . . . should qualify for exemption from the requirements of certain provisions of this Directive.' Moreover, Article 9 of the DPD creates an obligation for member states to adopt, in their national laws, exemptions or derogations from the provisions of chapters II, IV, and VI for the processing of personal data carried out solely for journalistic purposes or for the 'purpose of artistic or literary expression'. Such exemptions must, however, be 'necessary to reconcile the right to privacy with the rules governing freedom of expression'. Furthermore, the e-Commerce Directive recognizes that 'The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression'.[18]

With regard to liabilities for the illegal processing of personal data, the provisions of the DPD need to be coordinated with those of the e-Commerce Directive, which establishes, as we shall see, some exemptions for

11 There are some sectoral rules which regulate the protection of personal data in the private sector, such as, for example, the Fair Credit Reporting Act.

12 Article 6 TEU.

13 Article 8(2) of the Charter: '2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.'

14 Mandy Webster, *Data Protection in the Financial Services Industry* (Gower Publishing Limited, 2006) 109.

15 Case C-70/10 *Scarlet v SABAM* [2011].

16 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 [1995] OJ L281/31.

17 See, for instance, the Italian and the French data protection laws.

18 Recital 9.

ISPs when they transmit, host, or cache user-generated content. The most recent European legislation seems to confirm the need to limit the liability of the provider. Indeed, Directive 2009/136/EC,[19] amending the Universal Service Directive,[20] the Directive on privacy and electronic communications,[21] and the Regulation on consumer protection cooperation[22] reaffirm that the provider cannot be liable for merely transmitting user-generated information (the 'mere conduit' rule) and that it is not a provider's task to define what is lawful or harmful as to content, applications, and services.[23]

The European courts, such as the ECJ and the ECtHR, have set some general parameters for data protection law, and for the resolution of conflicts between privacy rights and the right to freedom of expression.

As to ECJ, the landmark *Lindqvist* judgment of 2003 addressed the application of the DPD to personal data posted on Internet websites.[24] Ms Lindqvist, who worked as catechist for a parish in Sweden, set up Internet pages for parishioners preparing for a sacrament. In those pages she provided information about herself and 18 fellow parishioners-catechists, indicating full names, jobs, hobbies, phone numbers, and other matters. Ms Lindqvist posted health related information about a person who had injured her foot and consequently worked half time on medical grounds.

The ECJ held that the act of mentioning, on an Internet page, individual persons, identifying them by name, and giving information about them, constitutes processing of personal data.[25] Moreover, according to the ECJ 'the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people'[26] is not covered by the exception provided for by Article 3(2) of the DPD, which only excludes from data protection the data-processing activities carried out in the course of the private or family life of individuals.

This judgment also addressed the relation between the DPD and the general principles of EU law, in particular, the fundamental rights enshrined in the European Convention of Human Rights, such as freedom of expression in particular. The ECJ stated that member states have a margin of manoeuvre in implementing the DPD, and emphasized the role of national jurisdictions,[27] stating that 'it is for the national courts to ensure a fair balance between rights and interests in question, including the fundamental rights protected by the European order.'

The *Lindqvist* judgment provides a useful framework for understanding how data protection rights can be applied even when no economic activities are involved. Excluding charitable and religious activities from data protection would have made the application of the DPD very uncertain, depending on the qualification of the concerned activity. The narrow interpretation given to the private or family life exception is particularly relevant, since it implies the application of data protection to individual users posting online information. We then need to establish how to apply the same data protection rules to two very different kinds of data controllers: on the one hand *bone fide* individuals, namely, users processing personal data for their individual purposes, and, on the other hand organizations processing personal information on large scale for commercial purposes.

For the judicial development of the data protection law, the *K.U. v Finland* judgment of the ECtHR is also very important.[28] It limits the duty/right to confidentiality of Internet service providers (and the protection of the privacy of their users), for enabling the protection of the rights of third parties and the prosecution of wrongdoings. The applicant was a

19 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.

20 Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services [2002] OJ L108/51.

21 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11.

22 Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2004] OJ L364/1.

23 Recital 31 of Directive 2009/136/EC: 'In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful. The Framework Directive and the Specific Directives are without prejudice to 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), which, inter alia, contains a "mere conduit" rule for intermediary service providers, as defined therein.'

24 Case C-101/01 *Lindqvist*[2003] ECR I-12971. See Jacqueline Klosek, 'European Court Establishes Broad Interpretation of Data Privacy Law'(2004) Findlaw, available at <http://library.findlaw.com/2004/Mar/19/133351.html> accessed 20 November 2011.

25 *Lindqvist*, para. 27.

26 Ibid, para. 47.

27 Ibid, para. 85.

28 *K.U. v Finland*, Judgment of 2 December 2008, application no. 2872/02.

12-year-old boy, who complained that an unknown person had, without his knowledge, placed an advertisement in his name on a dating site. The advertisement contained personal information of the applicant (name, phone number, link to personal page with photo, and description of physical aspects) and had a sexual connotation. The applicant became aware of the advertisement when somebody contacted him for a meeting.

The Internet service provider refused to reveal the identity of the IP address-holder, as it was bound by a duty of confidentiality according to Finnish telecommunications law. The Helsinki district court refused to oblige the service provider to disclose identification data in breach of professional secrecy, since there was no explicit legal provision authorizing the disclosure. More precisely, according to that court, malicious misrepresentation was not an offence authorizing the police to obtain telecommunications identification data. Other domestic courts upheld this position. The final result was that the applicant never got access to the identity of the person in question, and the managing director of the Internet service provider could not be prosecuted.

The Strasbourg court found that this outcome violated the right to private life, as defined in Article 8 of the ECvHR, 'a concept which covers the physical and moral integrity of the person'.[29] The right protected by Article 8 does not lead merely to a negative obligation on the state, but might also entail a positive obligation 'inherent in an effective respect for private or family life'.[30] According to the Court, 'these obligations might involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals among themselves'.[31] While States have a margin of appreciation in fulfilling the obligation arising from the Convention, the latter nevertheless places limits on this margin of appreciation. The Court, while acknowledging that 'freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others'.[32]

The scope of personal data rules has also been litigated at domestic level: a controversial example is represented by the UK case of *Durant v Financial Services* Authority.[33] This case concerned a person's request to have access to the files containing information about litigation he had with his bank (information detained by the Financial Services Authority). The request was rejected by the British Court of Appeal, which did not consider the information at issue to constitute 'personal data', ruling that personal data are only information which is 'biographical in a significant sense; has to have the individual as its focus; and has to affect an individual's privacy whether in his personal family life, business or professional activity'.[34]

It seems to us that the framework we have described, while still being under development, shows the emergence of some general principles, which also apply to the processing of user-generated data. These principles involve (a) the application of the data protection legislation to user-generated content distributed over the Internet; (b) the need to balance data protection rights of third parties with the freedoms of the users-uploaders; and (c) the exemption of liability for providers, an exemption which is strictly limited to user-generated content and is conditional on the provider's availability to cooperate with the concerned authorities, removing the material when requested. The ramifications of such principles will be considered in the following sections of this article, with regard to case law addressing videos and photos containing third parties' information posted on YouTube and Facebook-like websites.

Liability exemptions for ISPs in the e-Commerce Directive: the principle of neutrality

Article 2 of the e-Commerce Directive, borrowing the definition contained in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC,[35] considers a service provider as any natural or legal person delivering 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'[36] and a recipient of

29 Ibid, para. 41.
30 Ibid, para. 42.
31 Ibid, para. 43.
32 Ibid, para. 49.
33 *Durant v FSA* [2003] EWCA Civ 1746, Court of Appeal (Civil Division). For a comment, see Lilian Edwards, 'Taking the "Personal" Out of Personal Data: Durant v FSA and its Impact on the Legal Regulation of CCTV' (2004)1 (2) SCRIPT-ed.
34 Boštjan Berčič and Carlisle George, 'Identifying Personal Data Using Relational Database Design Principle' (2008) 17 International Journal of Law and Information Technology 223, 224.
35 In the same sense is Recital 17 of the e-Commerce Directive.
36 Article 2(a) of the e-Commerce Directive.

services as 'any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible'.[37]

For the purposes of analysing the liability of ISPs for user-generated content, the activity to be taken into account consists in hosting. The definition provided for by Article 14 of the e-Commerce Directive comprises an information society service 'that consists of the storage of information provided by a recipient of the service'. In that situation, the Directive exempts the ISPs from liability regarding the content generated by users under two conditions: (a) the provider has no actual knowledge of the illegal information or (b) it acts expeditiously to remove or to disable access to the information after obtaining such knowledge.[38]

According to recital 42 of the e-Commerce Directive, exemptions from liability cover only cases where the activity of the ISP 'is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge nor control over the information which is transmitted or stored.'

The ECJ has interpreted these provisions in the case *Google v Louis Vuitton*,[39] a preliminary reference raised from the French *Cour de Cassation*. Here is how the ECJ characterized the role of the host provider:

> It follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'.[40]

According to the Court, the neutrality of the provider provides the basis for the exemption from liability:

> Accordingly, in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.[41]

The idea that neutrality provides the decisive clue to address such cases has been contested by Advocate-General Jääskinen in his opinion in the case *L'Oreal v* eBay,[42] recently decided by the ECJ,[43] a case concerning the use of L'Oreal's trademark in the sale of counterfeited goods. While affirming the necessity to exempt ISPs from liability, the Advocate General denies that 'neutrality' is the right test under the directive. He argues that he 'would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding storage of information uploaded by the users.'[44] According to the Advocate General, the courts should not 'sketch out parameters of a business model that would fit perfectly to the hosting exemption',[45] since such an attempt would probably be very soon outdated. Advocate General Jääskinen proposes, instead, focusing on types of activity 'and clearly state that while certain activities by a service provider are exempt from liability, as deemed necessary to attain the objectives of the directive, all others are not and remain in the 'normal' liability regimes of the Member States, such as damages liability and criminal law liability.'[46] Therefore, for the case of eBay, the hosting of information generated by a client may benefit from the exemption provided for by Article 14 of the e-Commerce Directive. Nonetheless, Article 14 would not 'exempt eBay from any potential liability it might incur in the context of its use of a paid Internet referencing service'.[47] It seems to us the interpretation of the providers' exemption given by Advocate General Jääskinen does not necessarily contradict the idea of neutrality broadly understood, which does not require the inertia of the provider, but rather, covers any activity meant to enable or facilitate the initiatives in which the user autonomously engages on his or her own behalf. We must indeed consider the specific user's activity enabled by an ISP, and consequently understand neutrality as appropriateness with regard to the purpose of that user's activity.

37 Ibid, Article 2(d).

38 Article 14(a)(b) of Directive 2000/31/EC.

39 Joined Cases C-236/08, C-237/08 and C-238/08 [2010] *Google France, Google, Inc. v Louis Vuitton Malletier*, OJ C134, 22.5.2010, 2.

40 Para. 113. See Paul Przemyslaw Polanski, 'Technical, Automatic and Passive: Liability of Search Engines for Hosting Infringing Content in the Light of the Google ruling' (2011) 6(1) Journal of International Commercial Law and Technology 49, stating: 'In summary, the Court has accepted under certain conditions the extension of the sphere of application of Article 14 to sponsored links services. This is an important verdict as many third-party content service providers will now be able to rely on the lack of knowledge or control over data argument to avoid liability'.

41 Para. 114.

42 Advocate General Jääskinen, Opinion on the case Case C-324/09 *L'Oreal v Google*, para. 145.

43 Case C-324/09 *L'Oreal v Google*, OJ C 269, 10.09.2011, 3.

44 Advocate General Jääskinen (n 43), para. 146.

45 Ibid, para. 149.

46 Ibid, para. 149.

47 Ibid, para. 151.

The possibility to understand, in this broad way, the idea of neutrality is confirmed in the ECJ decision in the *eBay* case. The Court considered that an operator of a marketplace does not enjoy the exemption from liability under the directive on electronic commerce only when the operator takes an active role,[48] which presupposes knowledge of or control over the stored data.[49] According to the Court, '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'.[50] Only when 'the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.'[51] Thus, in this decision, the Court viewed the neutrality principle as the essential requirement for benefiting from the exemption of liability contained in the e-Commerce Directive.[52]

Having concluded that 'neutral' activities of the host provider are in general exempt from liability, according to EU law, we need now to consider whether there is a special discipline for data protection, so that neutral activities would also lead to liability when enabling violations of data protection. This conclusion seems to follow from Article 1(5)(b) of the e-Commerce Directive (Directive 2000/31/EC), which states that the Directive itself does not apply to 'questions relating to information society services covered by Directive 95/46/EC', an idea which is anticipated in Recital 14.[53] Thus, Article 1(5)(b) could lead to the conclusion that the safe harbour clause of the e-Commerce Directive does not apply to data protection, so that an ISP would be responsible for users' generated violations of third parties' data protection even when the ISP has only engaged in neutral activities.

However, we argue for a uniform approach to the ISP liability, and therefore the inclusion of data protection in the ISP exemption, on various grounds. First of all, various legislative materials, preceding and following the e-Commerce Directive, support this interpretation. In particular, in 1997 the European Parliament, in its resolution on the European Commission communication on a European Initiative in Electronic Commerce, recognized 'the horizontal nature of the liability problem, covering diverse issues such as copyright, consumer protection, trademarks, misleading advertising, protection of personal data, product liability, obscene content, hate speech, etc.'[54] Similarly, in its first report on the application of the e-Commerce Directive, the Commission states that 'The limitations on liability provided for by the Directive are established in a horizontal manner, meaning that they cover liability, both civil and criminal, for all types of illegal activities initiated by third parties.'[55]

48 *L'Oreal v Google*, para. 123.

49 See Mario Viola de Azevedo Cunha and Danielle da Costa Leite Borges, 'O caso Google-Louis Vuitton: a responsabilidade dos motores de busca por violações de propriedade intelectual e pela prática de delitos', Nota de Ensino, Casoteca Latino-americana de Direito e Política Pública (Escola de Direito de São Paulo da Fundação Getúlio Vargas—forthcoming).

50 *L'Oreal v. Google*, para. 115.

51 Ibid, para. 116.

52 See para. 119, stating: 'In situations in which that provider has confined itself to a merely technical and automatic processing of data and in which, as a consequence, the rule stated in Article 14(1) of Directive 2000/31 applies to it, it may none the less only be exempt, under paragraph 1, from any liability for unlawful data that it has stored on condition that it has not had 'actual knowledge of illegal activity or information' and, as regards claims for damages, has not been 'aware of facts or circumstances from which the illegal activity or information is apparent' or that, having obtained such knowledge or awareness, it has acted expeditiously to remove, or disable access to, the information.'

53 Recital 14 states:'The protection of individuals with regard to the processing of personal data is solely governed by 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(19) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(20) which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.'

54 European Parliament, Report on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce (COM(97)0157—C4-0297/97), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP// TEXT+REPORT+A4-1998-0173+0+DOC+XML+V0//EN&language=MT#top> accessed 23 February 2011.

55 Commission of the European Communities, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. First Report on the application of 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). Available at <http://eur-lex.europa.eu/

More recently, the Article 29 Working Party in its opinion concerning online social networking affirmed that when users go beyond a purely personal or household activity (such as when they use 'other technology platforms to publish personal data on the web') they become data controllers. Thus, users are subject to data protection obligations, and in particular they have to collect the consent from the data subjects whose information (or images) they are making available on the Internet.[56] The service provider is then required to inform the users of the privacy risks their behaviour may cause as well of their data protection obligations. Since users take on the role of controllers, deciding what data are to be processed in what ways, it seems that providers should not be liable for such choices of the users. This is in line with the recommendations made by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on its recently published report, where he affirms that 'censorship measures should never be delegated to a private entity, and that no one should be held liable for content on the Internet of which they are not the author.'[57]

Recently the ECJ adopted a similar position in the *Scarlet v Sabam* case, concerning an injunction to an ISP (Scarlet), to prevent its users from sending or receiving protected content. According to the judges, 'Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP which requires it to install the contested filtering system.'[58] In fact, 'the injunction in question would require Scarlet [the ISP] to actively monitor all the data relating to each of its customers in order to prevent any infringement of intellectual-property rights', that 'would impose general monitoring, something which is incompatible with the e-Commerce Directive.'[59]

It is our opinion that the text of Article1(5)(b) of the e-Commerce Directive can be reconciled with the sources just mentioned by interpreting it as concerning only the processing of personal data carried out by the host provider itself, on its initiative. Providers may indeed (and do often) violate EU data protection requirements by collecting or transmitting personal data concerning users or third parties without the consent of the data subject or in any case beyond the limits established by the law. Article 1(5)(b) makes it clear that in such cases ISPs cannot claim any exemption from liability resulting from e-commerce activities; they are thus responsible for all violations they commit by illegally processing personal data, for any initiative that violates the interests and the rights of users and third parties. The cases we are considering, however, pertain to a different issue, namely, to the liability of providers for illicit information about third parties uploaded by their users.[60] These considerations also apply to national legislation. In line with this interpretation, two of the authors of this paper in earlier research[61] have concluded that Italian legislation may be interpreted in such a way that the provider's exemption from liability also covers the online distribution of user-generated contents that are illegitimate because of the violation of data protection rules. It is true that Italian law apparently says that the exemption granted to providers does not apply to data protection rules, but it may be argued that this limit only concerns data collected by the provider for its own purposes, and not to data uploaded by the users.

As we shall see in the following review, the case law of different countries, in the EU and outside of it, seems indeed to support the contention that ISPs enjoy an exemption from liability for user-generated content also with regard to data protection violations.

A review of cases on ISP liability, user-generated content, and data protection

In this section, we will consider how different jurisdictions have addressed the liability of ISPs for user-generated content, with a special focus on violations of third parties' privacy. We shall mainly consider EU member states, in particular France and the Netherlands, but will also briefly refer to selected non-EU states (Brazil and the United States).

LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF> accessed 23 February 2011, 12.

56 Article 29 Working Party, 'Opinion 5/2009 on online social networking' (WP 163, 12 June 2009).

57 United Nations (n 5), at 13.

58 Case C-70/10 *Scarlet v SABAM* [2011], para. 54.

59 Court of Justice of the European Union, Press Release no. 126/11, 24 November 2011, 'EU law precludes the imposition of an injunction by a national court which requires an Internet service provider to install a filtering system with a view to preventing the illegal downloading of files'. Available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf>(last accessed December 5, 2011). The press release states: 'Such an injunction does not comply with the prohibition on imposing a general monitoring obligation on such a provider, or with the requirement to strike a fair balance between, on the one hand, the right to intellectual property, and, on the other, the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information'.

60 Giovanni Sartor and Mario Viola de Azevedo Cunha (n 4), at 21.

61 Ibid.

France

France is the European country having the highest number of decisions on user-generated content. Most of such cases concern copyrighted materials posted by users, but some of them also deal with violations of privacy. We will analyse here some of these cases (all translations are by the authors).

According to the French law on e-commerce, host providers are not be liable for user-generated content, unless they fail to act expeditiously once informed.[62] The victims of violations caused by user-generated content can notify the ISP to exclude the contested content, but a valid notification must contain very detailed information, including the legal provisions violated.[63] French law, in contrast to Italian law, does not include any provision excluding data protection from e-commerce regulation. However, French courts have showed uncertainty about applying the ISPs' liability exemptions for illegal user-generated content.

The exemption was upheld in a case, *Dargaud Lombard, Lucky Comics v Tiscali Média*, involving the posting without authorization of copyrighted publications, decided in 2005 by the *Tribunal de grande instance de Paris*, a lower court of general jurisdiction for civil matters.[64] The Tribunal concluded that an ISP can enjoy the exemption (being a host provider, rather than a content provider) even when it offers to its users the technical means to create their own web pages and to post materials (even copyrighted ones). Nevertheless, the *Cour d'appel de Paris* (an intermediate appellate court) overruled this decision in 2006, considering the ISP as a publisher (content provider), since it made profit through advertisements in the web pages containing the infringing materials, although the advertisements did not relate to such materials.[65]

In a subsequent case, *Jean Yves L. dit Lafesse v Myspace*, decided in June 2007, this time related to the posting of copyrighted videos, the *Tribunal de grande instance de Paris* followed the approach of the *Cour d'Appel*, concluding with regard to the ISP that 'in effect, by imposing a structure for presentation through frames, which it makes available to users and by promoting advertisements during every consultation, from which it clearly makes profit, it has the status of a publisher and should be liable' for infringing materials posted by users.[66]

In July 2007, the *Tribunal de grande instance de Paris* decided a case, *Christian C. v Dailymotion*, again involving the posting of copyrighted videos by users. It affirmed that the mere fact of profiting from advertisements in the web pages containing the infringing materials does not transform a host provider into a content provider. However, the Court condemned the provider (Dailymotion, a YouTube-like site), concluding that an ISP is liable for providing an infrastructure and technical means intended to enable the infringement (although the Court recognized that there is no duty of surveillance).[67] This decision was overruled by the Court of Appeal, which this time changed its view, affirming that the ISP was only providing a hosting service, since the fact of profiting through advertise-

62 Article 6.I.2 of the Loi n° 2004–575 du 21 juin 2004 pour la confiance dans l'économie numérique (French Act 2004–575 of 6 January 1978 on data Processing, Data Files and Individual Liberties).

63 The relevant provision states: '5. La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants:

- la date de la notification;
- si le notifiant est une personne physique: ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance; si le requérant est une personne morale: sa forme, sa dénomination, son siège social et l'organe qui la représente légalement;
- les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social;
- la description des faits litigieux et leur localisation précise;
- les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits;
- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.'

64 Tribunal de grande instance de Paris 3ème chambre, 1ère section, Jugement du 16 février 2005, *Dargaud Lombard, Lucky Comics / Tiscali Média*, available at <http://www.legalis.net/jurisprudence-decision.php3?id_article=1420> accessed 26 February 2011. In this case the court found the ISP liable for not having provided the necessary information to allow the copyright owners to identify the infringers.

65 Cour d'appel de Paris 4ème chambre, section A, Arrêt du 7 juin 2006, *Tiscali Media / Dargaud Lombard, Lucky Comics*, available at <http://www.legalis.net/jurisprudence-decision.php3?id_article=1638> accessed 26 February 2011. See 'La cour d'appel est la juridiction du second degré qui examine des affaires précédemment soumises à un tribunal lorsque le jugement ne satisfait pas une ou plusieurs parties au procès', available at <http://www.ca-paris.justice.fr/index.php?rubrique=10977&ssrubrique=11056> accessed 26 November 2011. A similar conclusion was adopted by the Tribunal de Grande Instance de Naterre in two cases decided on 28 February 2008, both of which involved a violation of private life. See Tribunal de Grande Instance de Nanterre, *Olivier D. / Aadsoft Com*and *Olivier Dahan / Eric* Duperri,available at <http://www.legalis.net/jurisprudence-decision.php3?id_article=2260> and at <http://www.juriscom.net/documents/tginanterre20080228.pdf> accessed 26 February 2011.

66 Tribunal de grande instance de Paris, Ordonnance de référé, 22 juin 2007, *Jean Yves L. dit Lafesse / Myspace*, available at <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1965> accessed 26 February 2011. This decision was considered void by the Paris court of appeal on the grounds of lack of summons. France: Cour d'appel de Paris, 14ème chambre, section A, Arrêt du 29 octobre 2008, *Myspace / Jean Yves Lafesse et autres*, available at <http://www.legalis.net/jurisprudence-decision.php3?id_article=2471> accessed 26 February 2011.

67 Tribunal de grande instance de Paris 3ème chamber, 2ème section. Jugement rendu le 13 Juillet 2007, *Christian C. / Dailymotion*,available at <http://www.juriscom.net/documents/tgiparis20070713.pdf> accessed 26 February 2011.

ments does make the ISP into a publisher (content provider).[68] Furthermore, the Court of Appeal affirmed that the ISP only has the obligation to exclude content if the 'victim' informs the ISP of all the details needed to identify the infringing material. The *Cour de Cassation* (the highest court in the French judiciary) affirmed this decision on 17 February 2011.[69]

The same *Tribunal de grande instance de Paris*, in a decision of 19 October 2007, *Zadig Productions v Google*, concerning the posting of a copyrighted documentary by a user, did not considered Google, the ISP, to be a content provider. Nonetheless, the court condemned Google for having failed to adopt measures preventing the re-posting of the documentary, stating that once an ISP is informed about the illegality of a specific content by a notification from the 'victim', it must implement all necessary measures to prevent further dissemination of the illicit material.[70] The same approach was adopted in another case against Google (*Flach Film v Google*),[71] this time decided by the *Tribunal de commerce de Paris*, a lower court specializing in trade and business matters.

The issue of the provider's liability for user-generated content violating privacy rights of third parties was addressed in a case, *Jean-Yves L. Dit Lafesse / DailyMotion*, decided by the *Tribunal de grande instance de Paris*, against Dailymotion.[72] The Court affirmed that an ISP should not be considered liable for the publication of videos making undue use of the image and name of a person; only the users who posted the videos should bear responsibility. Contrary to the approach adopted in the previous case *Zaig v Google*, the Court concluded that the 'victim' of illicit or infringing content has a duty to notify the ISP, providing all necessary information regarding the infringing content, to allow the ISP to identify it amongst the materials posted on its website. According to the Court, the victim has to give 'a description of the facts and of their precise location and of the reasons for which the contents must be removed including the reference to legal provisions or facts.' Only after receiving such information can the ISP be liable for not excluding the contested content.

This conclusion was confirmed by the Paris Court of Appeal in a case (*Olivier v Bloobox Net)* where the plaintiff claimed that the ISP was liable for violations of his private life as a consequence of hyperlinks to, and titles of, news posted by the users.[73] The court affirmed that the activity of 'structuring and classifying information made available to the public according to a classification determined by the provider with the aim of facilitating the use of its service fits the storage mission of the host provider and does not give him the quality of publisher (content provider) since it is not the author of titles and hyperlinks'.

In conclusion, we can observe an evolution of the French case law on ISPs' liability for user-generated content. In their first decisions, the French courts did not apply the safe harbour clause to ISPs, considering that when ISPs provide the technical means enabling users to commit the infringements[74] or make profit through advertisements, they should be considered to be publishers (ie content providers) and, therefore, liable. In some more recent cases, the French Courts

68 Cour d'appel de Paris 4ème chambre, section A Arrêt du 06 mai 2009, *Dailymotion / Nord-Ouest production et autres*, available at <http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2634> accessed 26 February 2011.

69 Cour de cassation, 1ère chambre civile, Arrêt du 17 février 2011, *Nord-Ouest Production et autres / Dailymotion*, available at <http://legalis.net/spip.php?page=jurisprudence-decision&id_article=3104> accessed 26 February 2011.

70 Tribunal de grande instance de Paris 3ème chambre, 2ème section, Jugement du 19 octobre 2007, *Zadig Productions et autres / Google Inc, Afa*. available at <http://www.legalis.net/jurisprudence-decision.php3?id_article=2072> accessed 26 February 2011.

71 Tribunal de commerce de Paris 8ème chambre Jugement du 20 février 2008, *Flach Film et autres / Google France, Google Inc*, available at <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2223> accessed 26 February 2011. See 'Le tribunal de commerce tranche, de manière générale, les litiges entre commerçants ou entre commerçants et sociétés commerciales, et ceux qui portent sur les actes de commerce', available at <http://www.ca-paris.justice.fr/index.php?rubrique=11016&ssrubrique=11051&article=14732> accessed 26 November 2011.

72 Tribunal de grande instance de Paris, 3ème chamber, 1ère section, jugement rendu le 15 Avril 2008, *Jean-Yves L. Dit Lafesse / DailyMotion*, available at <http://droit-finances.commentcamarche.net/jurisprudence/cour-d-appel-2/1097506-tribunal-de-grande-instance-de-paris-chambre-civile-3-15-avril-2008-08-01371> accessed 26 February 2011. This same approach was adopted by the same *Tribunal de grande instance de Paris* in another case against Daylimotion decided on 15 April 2008. Tribunal de grande instance de Paris, 3ème chamber, 1ère section, jugement rendu le 15 Avril 2008, Omar SY / Daylimotion, available at <http://droit-finances.commentcamarche.net/jurisprudence/cour-d-appel-2/1097503-tribunal-de-grande-instance-de-paris-chambre-civile-3-;15-avril-2008-;08-;01375> accessed 26 February 2011. In this case the Court reaffirmed the position that the ISP is not liable for user-generated content and that the mere fact it makes profit from advertisements does not change its role of a host provider and that the user is the one liable for undue use of the name or image of third parties.

73 Cour d'appel de Paris 14ème chambre, section B, Arrêt du 21 novembre 2008, *Bloobox Net / Olivier M.*, available at <http://www.legalis.net/jurisprudence-decision.php3?id_article=2488> accessed 26 February 2011. In the first instance proceedings, the Tribunal de grande instance de Paris had decided that the ISP was liable for the user-generated content but this decision was overruled by the Court of Appeal. See Tribunal de grande instance de Paris, ordonnance de référé rendue le 26 mars 2008, *Olivier M. / Boobox Net*, available at <http://www.juriscom.net/documents/tgiparis20080326.pdf> accessed 26 February 2011.

74 Lilian Edwards and Charlotte Waelde, 'The Fall and Rise of Intermediary Liability Online' in: Lilian Edwards and Charlotte Waelde (editors), *Law and the Internet* (3rd edn Hart Publishing, 2009) 72.

seem to have changed their views, not making the ISPs liable for storing user-generated content,[75] even in cases dealing with third parties' privacy. In this latter line of cases, ISPs are only liable when they do not intervene after a notification by the users.

The Netherlands

Liability for user-generated content has also often been litigated in the Netherlands, a country having a service-based economy and a high-quality IT infrastructure. Let us first consider two cases concerning litigation among private persons for information posted in social networks. In the first case,[76] a couple of divorced parents went to court because the father posted pictures and videos of their 5-year-old son on Hyves, a Facebook-like social network very popular in the Netherlands. More precisely, the father made various materials available online at different times, some in the public part of his profile, some in the private part of it. Among several complaints, the mother argued that the father was misusing parental care and breaching the child's privacy, which needed special protection, considering that both parents were working (in the past and at the time of the proceedings) with socially vulnerable persons.

In the assessment of the judge, the mother was right in claiming that the privacy of the child had been violated by the publication of the information in the public part of the social network; but for the information posted in the private part of the father's profile, in principle only accessible to his friends, the judge did not find a violation of privacy, or any other legal violation. While this case concerns litigation between two individuals, where the role and function of the ISP is not even mentioned, it is interesting since it distinguishes the private and public parts of a user's page in a social network, and limits data protection to the latter.

In a second case,[77] the claimant, a lawyer, requested removal, rectification, and compensation for alleged damages caused by negative comments posted by a user in her Hyves profile. Among other negative comments, the user asserted that the lawyer was a convicted paedophile. The comments, deleted by the user herself after a maximum of 55 hours, had been posted in the chat section of the web, whose access is limited to user's 'friends' and 'friends of friends'; it is therefore an area to which in principle only a restricted number of people have access. The Court focused on the fundamental rights involved, namely, freedom of expression and right to honour and reputation, and balanced them in light of the factual circumstances. According to the Court, freedom of expression also includes talking in a negative way about a person, is limited by the right to honour and reputation. However, only the accusation of being a convicted paedophile infringed the lawyer's honour and reputation, as the other parts of the text posted referred to a conflict between the parties; therefore the comments were permissible value judgements. This case also did not involve the liability of an ISP.

The provider's liability was directly at issue in a subsequent case,[78] where an individual sued an ISP who refused to remove a movie from its website. The facts are the following: the ISP, GeenStijl (literally: 'no style'), operated two websites where users could publish movies. In 2007, a then 20-year-old girl was filmed at night in a public area of Amsterdam (Leidseplein), drunk with a friend. The video was realized through a montage in which several pictures and sound recordings taken from the original footage were repeated a number of times. In the movie the 'drunk' girl first asks the cameraman to go away and then she starts answering his questions, revealing details about her private life. The video was first (2007) published on the Internet by the cameraman/producer, and later (9 July 2009) Studenten-TV published the film on its own website. In the same month (16 July 2009) the movie was published by GeenStijl on its website (www.dumpert.nl). In the introductory text the girl is addressed by her first name. Upon request of the girl's lawyer, GeenStijl removed the film on 23 July 2009. On 24 July 2009 the girl brought suit against Studenten-TV, the cameraman, and GeenStijl, asking for the removal (and prevention of re-posting) of the movie and of any comments on it, and for damages. At the time when the girl started the lawsuit, the film had been watched about 200,000 times and several offending comments had been added.

The movie was removed, but on 9 September 2009 another website (www.campus.tv) reported the case, mentioning the girl, the movie published by GeenStijl,

75 Julien Taïeb, 'Prestataires techniques de l'Internet: le sens de responsabilités' (2008) Juriscom.net 3, available at <http://www.juriscom.net/documents/resp20080519.pdf> accessed 26 February 2011, stating '[l]'hébergeur ne pourrait devenir éditeur seulement parce qu'il organise son site de manière logique . . . . L'hébergeur ne saurait non plus engager sa responsabilité éditoriale parce qu'il tire profit de son activité d'hébergeur.'

76 Rechtbank Almelo, 15 October 2009, *Nederlandse Jurisprudentie Feitenrechtspraak* 2009—49, No. 489.

77 Gerechtshof Amsterdam, 23 February 2010, *Computerrecht* 2010—3, No. 75.

78 Rechtbank Amsterdam, 11 September 2009, [. . .] versus GeenStijl (GS Media B.V.), *Computerrecht* 2010—2, No. 38.

and the claim for damages, and published some declarations by the girl's lawyer. The day after (10 September 2009) the movie was once again placed on the websites of GeenStijl, with the name of the girl, and with information on the proceedings she started, and publication of the correspondence with her lawyer. Additionally, GeenStijl published the video once again, this time while obscuring the girl's face, arguing that they had to defend themselves. On the same day the cameraman granted copyright to GeenStijl.

The Court found GeenStijl liable, even though it was not the author of the video, since it had autonomously published it. GeenStijl was held liable also for the comments it placed on the website as well as for the comments of third parties it kept on its website after receiving the request of removal. The Court justified this conclusion by considering that GeenStijl both provided the opportunity to place comments and was the final publisher of its sites. For this reason, the Court rejected the argument presented by GeenStijl that its role in the posting of the video corresponded to a mere technical transfer of data.

The reasoning of the Court considers the connection between privacy and freedom of expression. As the girl is recognizable in both versions of the movie, the movie constitutes a portrait according to Article 21 of the Copyright Act, which prohibits the disclosure of a portrait without the consent of the portrayed person, whenever a reasonable interest prevents disclosure. Reasonable interests in the sense of Article 21 include the protection of the privacy of the portrayed person, and thus the legitimacy of the publication of a portrait involves balancing privacy and freedom of expression, with regard to the factual circumstances (Article 10 ECvHR). The court affirmed that freedom of expression is not absolute, but can be restricted (Article 10(2) ECvHR) if such a restriction, as in this case, is provided by law and is necessary in a democratic society to protect other interests, such as reputation and rights of others. Thus the court concluded that the rights of the girl had been violated, as demonstrated by the evidence of damage to her reputation. The removal of the video and comments were therefore justified and proportionate. As to the request of the girl for a ban on comments on the judicial proceedings, the Court thought that this went too far, since in this regard freedom of expression prevailed.

An important case decided by the District Court of Amsterdam[79] concerns pictures of the children of the Royal Family, namely young Princess Amalia and her cousins Anna and Lucas. The plaintiffs were Crown Prince Willem-Alexander and his spouse, Princess Máxima (for Princess Amalia), as well as his cousin Prince Maurits and his spouse, Princess Marilène (for Anna and Lucas). The defendant was VerenigingMartijn, an association which defines itself as a 'platform for discussion about paedophilia', fighting for the 'social and societal acceptance of child–adult relationships', which manages the website www.martijn.org. On 25 October 2007 a picture of Princess Amalia was posted on the forum of the website of the association, with the comment: 'Our royal house has produced a whole new generation of princes and princesses, and luckily so!'. The picture was taken from the Royal Family official website, which allows use of the pictures it contains upon certain conditions. On the same day the Kingdom's Communication Department (Rijksvoorlichtingsdienst, RVD) asked the Association Martijn to remove that picture from their website. The picture was removed from the forum, but other photos of Princess Amalia and her cousins Anna and Lucas were posted on a private part of the website. The Association reacted to a subsequent complaint by the lawyer of the royal family, affirming that the restricted-access section of the forum was accessible only to five persons, and therefore there was no violation of the princess's privacy or portrait rights.

The main claims concerned violations of both copyright laws and of privacy and portrait rights by the Association Martijn. The Court dismissed the copyright claim against the ISP, as the pictures under dispute were published by a user and not by the ISP. According to the Court, the association only provides a forum where members can, among other things, post pictures. The association did not post those pictures, nor can it be expected to know that with the publishing of a picture the copyright of a third person can be violated. It cannot be required that the owner or operator of a website should check the content of what is posted in a forum, in order to prevent possible breaches of law. The second claim concerned the violation of the right to privacy and of portrait rights. The Court found that it is undisputed that paedophilia as a sexual orientation is socially disapproved, public declarations of it are undesirable and exposure of children to paedophile behaviours is to be condemned. Nevertheless, freedom of expression, as protected by Article 10 of the ECvHR and by the Dutch Constitution (Article 7), protects the

79 Rechtbank Amsterdam, 1 November 2007, members of the Royal Family versus Vereniging Martijn, *Computerrecht* 2008—1, No. 8.

public debate over paedophilia. Therefore, according to the Court, the Association Martijn was entitled not only to divulge its opinions, but also to disseminate those of other persons, within the limits of the law. However, the Court affirmed that a person's privacy is violated when that person or his/her children get involved in the paedophilia debate, without them wanting to or there being a general interest requiring so. Consequently, the Court held that the publishing of a photo on a website such as the one under dispute, especially on the public forum, by connecting the child's picture to paedophile wishes and actions, constitutes an unacceptable violation of the privacy of the child and of her/his parents and violates the portrait right of the child.

The Court also considered that given the special nature of the website, the Association Martijn should have been aware the website could be misused (even relative to the standards of the association). For this reason, it could be expected that the defendant—unlike other owners or operators of websites that do not have to watch out for such misuse or unintended usage—should take adequate precautionary measures when operating the website and the forum. Such measures should make it impossible for persons who do not know the limits of their freedom of expression to use the website to make publications which violate the rights of others.

Therefore, the Court denied the application of the safe harbour clause[80] to the Association Martijn. It argued that the association selected the persons to whom it granted active access to the forum and used the forum to reach its own goals, so that the activity of Martijn could be deemed not to be mere 'hosting', but rather to constitute publishing.

The Association Martijn claimed it was excessive to require from it, a small organization, to 'police' its website from possible abuses. The Court rejected this argument, stating that organizational inability did not justify the violation of others' rights, and suggesting also some practical solutions, like setting up the forum in such a way that the contributions had to be accepted by a moderator before becoming visible. The delay of the publication of users' postings would not undermine the latter's right to freedom of expression. Such an obligation to exercise preventive control over the website, was, according to the Court, a legitimate limitation of freedom of speech, necessary to protect the rights of others.

In this case the Court affirmed that the provider was a content publisher, and therefore could not enjoy the 'safe harbour' status. On this point the reasoning of the Court seems questionable, since this approach (an ISP is responsible for the posted contents when it has control over the selection of the participants and has an interest in the discussed topic) could lead to the liability of whoever hosts or moderates a website dealing with social or political issues. However, another aspect of this decision is very interesting, namely, the view that the nature of the information hosted by a provider, and the kind of audience it addresses, may require that the provider takes a more active role, adopting special precautionary measures.

Other EU member states: Italy and Spain

The issue of the liability of ISPs for peer violations of data protection has also emerged in other EU member states, and different approaches have been adopted. We cannot provide here a comprehensive review, but we will mention two cases, one from Italy and one from Spain, as evidence of the ubiquity of this issue.

An Italian trial court judge in the case *Google v Vividown*[81] recently held three Google executives guilty for violating data protection law, in connection with the posting of a video showing a disabled person being bullied and insulted. The judge grounded the criminal conviction of the Google executives on the fact that Google processed the video without taking adequate precautionary measures to avoid privacy violations, and in particular without properly informing the involved users of their obligation not to post illegally personal information and in particular health data. The Italian judge made no explicit reference to the ISP's exemption from liability granted by the Italian Legislative Decree on e-commerce. Thus, contrary to the view we advanced in above, he seems to have assumed that the ISP exemption does not cover data protection, on the basis of a literal interpretation of Article 1.2.b of the same decree, which excludes from the e-commerce regulation any 'issues concerning the right to privacy

80 Article 6:196c of the Dutch Civil Code, implementing the safe harbour clause of the e-Commerce Directive.

81 'Tribunale in composizione monocratica (giudice monocratico)—È competente per tutti i delitti che non sono attribuiti al Tribunale in composizione collegiale o alla Corte di Assise (sono attribuiti al giudice monocratico i delitti in materia di traffico dì stupefacenti quando non ricorrono le aggravanti). Di regola, per i delitti di competenza del giudice monocratico, non è prevista l'udienza preliminare, ma si procede con citazione diretta al giudizio dell'imputato (cosa che avviene sempre per le contravvenzioni)', available at <http://www.ristretti.it/glossario/penale.htm#Tribunale%20in%20composizione%20monocratica> accessed 26 November 2011).

with regard to the processing of personal data in the telecommunications sector'.[82]

A different approach has been adopted in Spain, where the National Data Protection Authority, without mentioning the safe harbour contained in Article 16 of Law 34/2002 (which implemented the e-Commerce Directive), has affirmed that only users are liable for data protection violations as a consequence of images posted in YouTube.[83] The Spanish e-Commerce law, like the French one, does not make any reference to data protection law, and, in particular, does not contain any clause limiting its application on privacy grounds.[84]

Non-EU states: examples from Brazil and the USA

'Safe harbour' limits to ISPs' liability have been introduced not only in EU member states but also in other countries. Here we discuss two particularly significant cases from Brazil and the USA.

In Brazil, there is no general data protection legislation[85] nor is there any legislative safe harbour for ISPs. However, the Superior Court of Justice, the Brazilian highest court in non-constitutional issues, decided that Google was not liable in a recent case concerning offensive user-generated materials posted on a social network managed by Google.[86] According to the Court, Google has no duty to previously control the content posted by users because this control could lead to restrictions to freedom of expression. Nevertheless, the Court stated that as soon as the ISP is aware of the existence of illegal information on its websites it has an obligation to remove the information immediately.[87] In another case involving the posting of offensive materials in a social network managed by Google, the same Superior Court of Justice concluded that an ISP has no obligation to monitor the content posted by its users.[88] These decisions take the same line as the safe harbour clause contained in the e-Commerce Directive, according to a line of reasoning that could be applied to all cases involving violations of third parties' rights by user-generated content.

In the USA, the Digital Millennium Copyright Act (DMCA) contains safe harbours limiting the liability of ISPs regarding copyright infringements by user-generated content. The approach adopted by the USA is different from that of the EU, which 'expressly chose not to focus exclusively on copyright, but rather to tackle the issue of ISP liability in a so-called horizontal manner—that is, drafting the safe harbours to cover intermediaries' liability for any kind of unlawful content provided by their users, whether it constituted copyright infringement, trademark infringement, defamation, unfair competition, hate speech or any other type of illicit material.'[89]

Non-copyright related violations are addressed in the USA by the Communications Decency Act of 1996 (CDA), which states in its section 230(c) that 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider.'[90] This clause apparently also exempts providers from liability with regard to privacy violations through user-generated

82 Article 1.2.b of theDecreto legislativo 9 aprile 2003, n. 70Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno(ItalianLegislative Decree 70 of 9 April 2003), available at <http://www.interlex.it/testi/dlg0370.htm> accessed 25 February 2011.

83 See, for instance, <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00479-;2008_Resolucion-de-fecha-30-;12-;2008_Art-ii-culo-6.1-LOPD.pdf> and <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2009/common/pdfs/PS-00055-;2009_Resolucion-de-fecha-20-;07-;2009_Art-ii-culo-6.1-LOPD_Recurrida.pdf> accessed 25 February 2011.

84 Article 16.1 of Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (Spanish Law 34/2002 on information society services and electronic commerce), available at <http://noticias.juridicas.com/base_datos/Admin/l34-2002.t2.html#a16> accessed 25 February 2011.

85 The Brazilian Ministry of Justice recently launched a public consultation on a draft bill of law on data protection and privacy. See <http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf> accessed 26 February 2011.

86 'O STJ é a última instância da Justiça brasileira para as causas infraconstitucionais, não relacionadas diretamente à Constituição. Como órgão de convergência da Justiça comum, aprecia causas oriundas de todo o território nacional, em todas as vertentes jurisdicionais não-especializadas', available at <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=293> accessed 26 November 2011.

87 Superior Tribunal de Justiça, 'Google não pode ser responsabilizado por material publicado no Orkut', 20 January 2011, available at <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=100532> accessed 12 February 2011. A draft bill, which goes in a similar direction as the decision adopted by the Superior Court of Justice, is being analysed by the Brazilian Ministry of Justice and will be probably sent to the Parliament soon. See <http://www2.camara.gov.br/agencia/noticias/ COMUNICACAO/192871-CAMARA-DEVE-ANALISAR-NESTE-ANO-MARCO-CIVIL-DA-INTERNET.html> accessed 20 February 2011.

88 Superior Tribunal de Justiça, Recurso Especial nº 1.186.616—MG (2010/0051226-;3), available at <https://ww2.stj.jus.br/processo/jsp/revista/abreDocumento.jsp?componente=ATC&sequencial=17189288&num_registro=201000512263&data=20110831&tipo=5&formato=PDF> accessed 26 November 2011.

89 Miquel Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2009) 32 Columbia Journal of Law & Arts, 482. The article goes on to state that 'The rationale behind this approach appears to be that a service provider is carrying out the same technical activity—whether transmitting, caching or hosting third-party content—regardless of the type of content involved.' Ibid, at 482.

90 Available at <http://www.fcc.gov/Reports/tcom1996.txt> accessed 29 April 2011.

content.[91] As highlighted by Edwards, the CDA provides a broader exemption than the DMCA:

> [the DMCA] exempts ISPs from liability for hosting copyright infringing materials in a set of 'safe harbours', but only on certain terms, such as the disclosure of the identity of infringers on request, subscription to a detailed code of practice relating to notice, 'take down' and 'put back', and the banning of the identified repeat infringers from access. By contrast, section 230(c) of the Communications Decency Act (CDA) provides total immunity in respect of all kinds of liability bar relating to IP, so long as the content in question was provided by a party other than the ISP.[92]

Even before the adoption of the DMCA or of the CDA the US Supreme Court has applied, in the field of copyright law, the judicial 'safe harbour clause' which 'provides immunity from liability for technology that is "capable of substantial non infringing uses"'.[93] This happened in the famous case involving Sony, which at that time was producing the video recorder Betamax, where the Court considered that Sony 'could not be held liable for making technology that was capable of copying for fair use purposes.'[94]

Finally, we need to consider that content that would be considered illegal on data protection grounds in Europe would not be considered as such under US law, where freedom of expression usually takes precedence (unless copyright is involved). It also important to notice that US tort law in what concerns 'Public Disclosure of Private Facts'[95] requires that the privacy-invasive material has to be distributed to the public at large 'in the form of widespread dissemination that goes beyond mere "disclosure" or "publication" as these terms are understood in the law of defamation.'[96] Thus, for example, distribution of such materials on a local area network (LAN) might not satisfy the 'publication' requirement for the purpose of liability under the privacy torts involving publicity,[97] and the same holds with regard to distribution on a social network when the privacy-invasive material is shared with a limited group of users.'[98] Thus, in certain cases, the issue of the provider's liability for user-generated content would not even emerge, since the users themselves would not be considered liable. As an extreme example of this approach, we can mention the recent US state case *Lalonde v Lalonde*[99] concerning the use in a trial of one person's photos taken from Facebook, where they were published without her consent. The court allowed the use of the photos, stating that 'There is nothing within the law that requires her permission when someone takes a picture and posts it on a Facebook page. There is nothing that requires her permission when she was 'tagged' or identified as a person in those pictures.'[100]

Conclusions

The online publication of user-generated content including personal data directly concerns a conflict between the user posting the information and the data subject, and thus a conflict between the user's freedom of expression and the data subject's privacy and data protection rights. However, it also involves the ISP, on whose platform the content is published and distributed. As we have seen above, the role of the ISP can be construed in different ways.

On the one hand, the ISP may appear to be co-responsible to the violation of privacy: the ISP contributes the means through which the privacy violation is committed, and does that for a profit. Moreover, by making the information easily accessible and searchable the ISP enhances its illicit circulation.

On the other hand, the ISP has the role of an enabler, rather than that of an author, of the violations. In fact, by providing users with the possibility of free and uncensored use of its platform, the provider contributes, while aiming at a profit, to the free development of citizens personality, to the growth of civil and political debate, and to the creativity of the Internet.

The multifaceted role of ISPs, and the different legal values involved in their activity, explains why there is an on-going debate over whether and to what extent they should be liable for illegal user-generated contents, a debate that is likely to continue in the future. In EU law, which is the focus of this article, two conditions are required for the provider to block or remove illegal

91 Miquel Peguera (n 89), at 484.

92 Lilian Edwards, 'The Fall and Rise of Intermediary Liability Online' in Lilian Edwards and Charlotte Waelde (n 74), at 64.

93 See Edward Lee 'Decoding the DMCA Safe Harbors' (2009) 32 Columbia Journal of Law & the Arts, 233, 268.

94 Ibid, at 268.

95 On US tort law applicable to privacy violations, see William L. Prosser, 'Privacy' 48 (1960) California Law Review 383-;423.

96 Dorothy J. Glancy, 'At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet' (2000) 16 Santa Clara Computer and High Technology Law Journal 364.

97 Ibid, 6. This conclusion can be extracted from the case *Wood v National Computer Systems, Inc.*, 814 F.2d 544 (8th Cir. 1987), available at <http://openjurist.org/814/f2d/544/ wood-v-national-computer-systems-inc> accessed 26 December 2011.

98 See, for instance, *Bret Michaels v Internet Entertainment Group, Inc.*, 5 F. Supp. 2d 823 (C.D. Cal 1998), available at <http://www.Internetlibrary.com/pdf/ Michaels-Internet-Entertainment-Group.pdf> accessed 26 December 2011.

99 Kentucky Court of Appeal, 25 February 2011.

100 Available at <http://ky.findacase.com/research/ wfrmDocViewer.aspx/xq/fac.20110225_0000218.KY.htm/qx> accessed 29 April 2011.

content (so preventing the violation or its continuation): first of all, the provider must be aware that the user has carried out a certain activity, and secondly, he must obtain knowledge that the content generated by that activity violates someone else's rights (in particular privacy rights).

The first aspect has frequently been mentioned when considering whether to limit the liability of providers. So, it has often been affirmed that the provider cannot be made responsible since the provider cannot reasonably control all user-generated content. However, we think that the second aspect also needs to be considered. In fact, establishing that user-generated content is illegal often involves an uncertain balancing exercise: the legality of the distribution of the content depends on whether, under the particular conditions of the case, the uploader's civil rights (and in particular his or her freedom of expression) should prevail over the third party's privacy rights. By making the ISP responsible for the illegal content hosted in its platform, even without a request by a competent authority, we put the burden of establishing whether the content is illegal on the ISP. Thus there is a risk of favouring an excessively cautious attitude by the provider, who, to prevent possible liability, would indulge in censorship whenever there is the smallest risk of a judicial decision in favour of privacy, thereby unduly restricting freedom of expression.[101] There is also a risk that those who want to prevent the distribution of information about themselves will threaten to sue providers for privacy violation, to induce the providers to censor the concerned content, even when it expresses legitimate criticism.

This is the fundamental legal and political issue that underlies the more specific and apparently technical questions involved in this subject matter, namely the issues of whether the provider or the user is the data controller, of when online distribution can be considered to be a private activity (to which data protection is inapplicable) having limited accessibility, of whether and to what extent the liability exemption for host providers also concerns violations of privacy.

As discussed in this paper, it seems to us that even with regard to third parties' data protection, the current rules limiting the liability of host providers with regard to user-generated content give the most appropriate balance between the interests and the rights involved. This conclusion does not exclude the need for providers to take initiatives concerning the education of their users with regard to data protection. In particular, platform providers should be urged (by the competent data protection authorities) to provide their users with better information about the need for other people's privacy rights to be respected, as suggested by the Article 29 Working Party.[102] We think that such precautions would be fully consistent with the limitation of the provider's liability, since they do not impose any censorship on users, but are only meant to make them aware of their pre-existing data protection duties.[103]

Furthermore, a review of the e-Commerce Directive, in order to make clear that the exemptions of liability also apply to data protection, would be very welcome. We think that providers' liability of user-generated content is one of most significant issues to be addressed in the 'Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC)' recently launched by the European Commission.[104]

On 25 January 2012 the EU Commission has put forward a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),[105] aimed at revising Directive 95/46/EC. The proposal, which was drafted by DG Justice, has already been the object of criticism from other DGs. The Information Society and Media (INFSO) Directorate-General has stated in its response to the inter-service consultation on the proposal that 'the whole draft Regulation would have "significant negative effects" on the development of the digital economy and jeopardise the Commission's Digital Agenda.'[106] In particular, the proposal may be understood as making ISPs liable for user-generated content (in case the ISPs were considered data controllers with

101 United Nations (n 5), at 14, stating: 'To avoid infringing the right to freedom of expression and the right to privacy of Internet users, the Special Rapporteur recommends intermediaries to: only implement restrictions to these rights after judicial intervention; be transparent to the user involved about measures taken, and where applicable to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and minimize the impact of restrictions strictly to the content involved.'

102 Article 29 Working Party (n 56), at 7.

103 Giovanni Sartor and Mario Viola de Azevedo Cunha (n 3), at 23.

104 Available at <http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm> accessed 24 February 2011.

105 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 26 January 2012.

106 Information Society and Media Directorate General (INFSO), 'Reply to the Interservice consultation launched by DG JUST on the Proposal (draft) for a Regulation of the European Parliament and of the Council

regard to such content), since it states in its article 17(2) that 'Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.' INFSO has suggested that this should be removed altogether, since it is not clear what kind of authorization it is contemplating.

We think that any future data protection regulation should more generally clarify that host providers are not controllers with regard to the user-generated content, and that they are exempted from liability with regard to such content. For this purpose, INFSO suggests inserting the following paragraph in Aricle 17 of the proposal:[107] 'Service providers, other than controllers, acting only as conduits or merely providing automatic, intermediate and temporary storage or storage of information provided by a recipient of the service or allowing or facilitating the search of or access to personal data, shall not be responsible for personal data transmitted or otherwise processed or made available by or through them.'[108] We hope that these observations will be duly taken into account in the final text of the regulation.

doi:10.1093/idpl/ips001
Advance Access Publication 8 March 2012

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DP Regulation), Reference: DG JUST.C3 (2011) 1350739 bis', available at <http://www.edri.org/files/120112_DGINFSO_negativereply.pdf> accessed 26 January 2012, 4.

107 The INFSO response refers to Article 15 of the Draft Proposal distributed in the EU Commission interservice consultation, which corresponds to Article 17 of the Proposal.

108 Ibid, at 11.