# Editorial

With the recent Google v. Spain decision by the European Court of Justice[1] and the Delfi v. Estonia case before the Grand Chamber of the European Court of Human Rights (ECtHR),[2] the position of internet intermediaries is at the center of attention once again. In Google v. Spain, the ECJ decided that Google must be seen as the controller of the information it indexes. Hence, all legal obligations specified in the Data Protection Directive should be respected by Google and other internet intermediaries like it. In the Delfi v. Estonia, the ECtHR ruled that internet platforms running on User Generated Content and user comments can rely on the freedom of speech, protected under article 10 ECHR.[3] Still, this right may be curtailed if the rights of others are infringed through, for example, defamatory user comments. It is interesting to see that these two regimes are now applied to internet providers, while originally, the e-Commerce Directive from 2000[4] was meant to be the main juridical framework under which to judge the liability of internet intermediaries for actions conducted by their users through their networks.

The e-Commerce Directive contains so-called safe harbors, which exempt passive Internet intermediaries from liability under certain conditions. Firstly, Article 12 specifies that an access provider is not liable for the information transmitted, on condition that the provider (a) does not initiate the transmission, (b) does not select the receiver of the transmission and (c) does not select or modify the information contained in the transmission. Secondly, Article 13 regards providers engaged with caching, but this provision has been of almost no relevance in legal practice. Finally, Article 14 holds that a hosting provider is not liable for the information stored, provided that (a) the provider does not have actual knowledge of any illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent and (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. In addition, Article 15 provides that Member States may not impose a general obligation on intermediaries to monitor the information that they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

Since the introduction of the e-Commerce Directive, providers have become increasingly active, for example by indexing information and making it searchable, by creating social platforms and by maintaining sites that are based on User Generated Content. The question is whether these active Internet intermediaries can also rely on Article

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

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

3 European Convention on Human Rights, Rome, 4.XI.1950.

4 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce or the e-Commerce Directive).

14 of the e-Commerce Directive. Of course, this will not be the case with, for example, news sites that publish their own material, written by their own employees, on their own website.[5] They will be regarded as publishers rather than Internet providers. But the question is more difficult to answer with respect to intermediaries such as Facebook, Ebay, Youtube and news sites that run on User Generated Content. The ECJ appears to have answered the question affirmatively in its L'Oreal/Ebay ruling, which focused on illegal content posted by users on Ebay. The Court held in respect of Ebay that 'the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31.'[6] Still, it cannot 'rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31.'[7]

However, the e-Commerce framework is not the only regime that applies to the liability of internet intermediaries. It follows from Article 1 paragraph 5 sub b that the safe harbors do not apply to questions relating to information society services covered by the Data Protection Directive[8] and the e-Privacy Directive.[9] Recital 40 of the e-Commerce Directive holds that 'the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC [the Data Protection Directive] and 97/66/EC [the predecessor of the e-Privacy Directive].' These are notoriously vague provisions, but the ECJ case law shows that a distinction should be made between three types of cases. First, cases in which intermediaries are held liable for an infringement committed by a user through its network, for example, an intellectual property right: the e-Commerce Directive is applicable. Second, cases in which intermediaries are held liable for an infringement, committed by a user via its network, on a person's right to data protection: the Data Protection Directive is applicable. Third, cases in which an infringement of an intellectual property right has been initiated by a user and an Internet service provider is asked to provide the name and address of the user (that is to provide personal data) or to effectuate a monitoring system: both directives apply. In the latter instance, the ECJ will assess the case by relying on various directives, such as the e-Commerce Directive,



5 Court of Justice, Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis, case C-291/13, 11 September 2014.

6 Court of Justice, L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi, case C324/09, 12 July 2011, para. 115.

7 L'Oréal/eBay, para. 124.

8 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

9 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Directive 97/66/EC has been replaced by Directive 2002/58/EC and the references to the first directive must be read as a reference to the second directive.

the directives on data protection and the directives regarding the protection of intellectual property.[10]

If personal data are processed by internet intermediaries, the Data Protection regime will apply. Active Internet intermediaries will in principle be considered the controller of data within the meaning of the Data Protection Directive, as recently evidenced by the Google v. Spain judgment of the ECJ. In its search engine, Google had referred to a story in a newspaper, which had digitalized its archive and published it online. Mr Costeja González's name appeared in relation to a real-estate auction connected to proceedings for the recovery of social security debts. The content of the message itself was not illegal neither was the newspaper requested to remove the story from its paper archive or even from its website. The question was whether Google could be obliged to delete the link to the story from its search engine and related to that, whether it could be held responsible for processing personal data because it had indexed the material and made it possible to search the contents of the material. The Court held: 'It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing []'.[11]

The controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The controller is contrasted to the "processor", which is the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller. It follows, inter alia, that purely passive hosting providers, that neither determine the means nor the purpose of the data processing, will in principle not be considered the controller, but the processor of personal data. Therefore, they are not responsible for upholding the rights and duties under the Directive, the controller is. But apparently, active Internet intermediaries must be seen as full-fletched controllers and they are required to respect all the duties and obligations specified in the Data Protection Directive. Consequently, there seems to be a fundamental difference in comparison to the regime under the e-Commerce Directive, because even more active Internet intermediaries can, under certain conditions, invoke the safe harbors therein contained.[12]

But there is even a third regime that may apply to providers. Internet intermediaries may also rely on fundamental rights themselves. This was evidenced in the Delfi v. Es-

10 Court of Justice, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), intervening parties: Belgian Entertainment Association Video ASBL (BEA Video), Belgian Entertainment Association Music ASBL (BEA Music), Internet Service Provider Association ASBL (ISPA), case C-70/10, 24 November 2011. Court of Justice, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, case C360/10, 16 February 2012. Court of Justice, Productores de Música de España (Promusicae) v Telefónica de España SAU, case C275/06, 29 January 2008.

11 Google v. Spain, para. 33.

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

tonia judgement by the ECtHR. In the lengthy national proceeding, the website was sometimes treated as an Internet intermediary under the rules of (the implementation of) the e-Commerce Directive and sometimes as a journalistic news medium under the doctrine of freedom of expression, because the site was considered too active to qualify as a passive Internet intermediary. Both in the national proceedings and before the ECtHR, the latter vision ultimately prevailed, and the website was treated under Article 10 ECHR and not under the e-Commerce Directive. The argument of the Estonian government before the ECtHR on this point is interesting, as is the rejection of it by the ECtHR: 'The Government pointed out that according to the applicant company it had been neither the author nor the discloser of the defamatory comments. The Government noted that if the Court shared that view, the application was incompatible ratione materiae with the provisions of the Convention, as the Convention did not protect the freedom of expression of a person who was neither the author nor the discloser. The applicant company could not claim to be a victim of a violation of the freedom of expression of persons whose comments had been deleted. (...) The Court notes that the applicant company was sued for defamation in respect of comments posted on its Internet portal, it was deemed to be discloser (...) of the comments – along with their authors – and held liable for its failure to prevent the disclosure of or remove on its own initiative the unlawful comments.'[13] From this, the ECtHR concluded that the provider was curtailed in its right to expression. This was confirmed on 16 June 2015 by the Grand Chamber.[14]

In particular, the ECtHR felt that the measures taken by Delfi, i.e. the terms and conditions which prohibited defamatory comments, the notice and takedown system, the monitoring activities and the automatic filter system it employed, were insufficient. Although these measures go beyond what is necessary for the duty of care under Article 14 e-Commerce Directive, they are apparently insufficient when it comes to the duty of care under Article 10 ECHR. A salient detail is that the Court ruled that it was legitimate to hold Delfi liable, while not even trying to press charges against the actual authors of the comments, because Delfi allowed them to post comments anonymously. 'It notes that it was the applicant company's choice to allow comments by non-registered users, and that by doing so it must be considered to have assumed a certain responsibility for these comments.'[15] This is remarkable because the ECtHR also agrees that the ability to post comments in full anonymity is an important part of both the right to privacy, the right to data protection and the right to freedom of expression, while the efforts to that end of Delfi bring with them that it runs a higher risk of being held liable for the comments of users than if it would not have allowed anonymous reactions.

Consequently, roughly three regimes may now apply to internet intermediaries with regard to the liability for privacy violations on third parties' rights conducted by their

13 Delfi v. Estonia (first instance), paras. 48 and 50.

14 Delfi v. Estonia (Grand Chamber).

15 Delfi v. Estland (first instance), para. 91.

users through their networks. This has complicated matters substantially. For active intermediaries, the data protection regime is substantially different from the e-Commerce regime. The Data Protection Directive imposes many duties on active Internet intermediaries, and this burden will only be intensified when the General Data Protection Regulation is adopted. As a result, active Internet intermediaries can rely on the exclusion of liability under the e-Commerce regime much more quickly than under the data protection regime. And providers may also rely on the freedom of expression, for the protection of their own interests, even if they are considered responsible for illegitimate actions of the users of their services conducted through their network. It should also be noted that the regimes of the European Union, including that of the e-Commerce Directive and the Data Protection Directive, and the instruments of the Council of Europe, including the ECHR, deviate on a number of points. This is reinforced by Article 8 ECHR, which also provides partial protection to private property and against criminal acts, while these matters are treated under the e-Commerce Directive rather than the Data Protection Directive in EU law. Article 8 ECHR also covers the right to reputation and rules on data protection, but the latter right is treated and explained in substantially different terms by the ECtHR than by the ECJ.[16]

In conclusion, while the e-Commerce Directive was installed to clarify the position of and to provide greater legal certainty to providers (given the great diversity in national rules that existed before the entry into force of the Directive), it has to be acknowledged that the current situation in Europe regarding the liability of Internet intermediaries is still very diffuse and unclear. Despite the rules contained in the Directive, countries in Europe have a very different take on many of the complex questions and positions. Courts and judges will often have a very wide margin of appreciation and thus responsibility for weighing and balancing the different interests and positions involved. Also, Internet intermediaries themselves have an important role in balancing the various interests and circumstances of the case, and this creates an even more diffuse picture, because of the different attitudes and approaches by the various providers. As in Europe, in contrast to for example the American Digital Millennium Copyright Act, no legislative framework exists for the handling of requests by third parties and these requests are often handled by providers before a case is judged by a court of law, Internet providers often have to make an assessment of the case independently and assume the role of a judge. Providers have to judge under which regime the claim falls, they must determine correctly their own position, they must determine correctly the validity of the claim of the third party, they must balance the third party's interest to, for example, copyright against the user's right to, for example, the right to data protection and the freedom of expression. It must also assess its own role, and determine whether it has adopted sufficient duties of care as specified in the various regimes and finally, it must also take into account its own right to freedom of expression and possibly the freedom to conduct business, as enshrined in Article 16 of the EU Charter of Fundamental Rights. Although revision of the e-Commerce Directive has been discussed for

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

years, perhaps now is the time to formulate a unified approach to the liability of Internet providers for privacy violations in Europe.[17]

The role of recent case law on Internet intermediaries is also the topic of the contribution '*Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain',* written by Stefan Kulk and Frederik Zuiderveen Borgesius. They argue that since the Google Spain judgment, Europeans have, under certain conditions, the right to have search results for their name delisted. They examine how the Google Spain judgment has been applied in the Netherlands. Since the Google Spain judgment, Dutch courts have decided on two cases regarding delisting requests. In both cases, Stefan and Frederik argue, the Dutch courts considered freedom of expression aspects of delisting more thoroughly than the Court of Justice. But they also concede that the effect of the Google Spain judgment on freedom of expression is difficult to assess, as search engine operators decide about most delisting requests without disclosing much about their decisions.

The other article, entitled *The Proposed Data Protection Regulation and its Potential Impact on Social Sciences Research in the UK*, is by Leslie Stevens. In that article, Leslie critically assesses the potential impact of the proposed Data Protection Regulation on the undertaking of social sciences research in the UK, providing practical analysis from the perspective of research involving administrative data. This assessment reveals how changes to the key concepts of anonymisation, personal data, and lawfulness may impact upon social sciences research. The approach taken in drafts to the proposed Regulation, Leslie argues, represents a disproportionate and de-contextualized response to the risks involved in undertaking social sciences research that may create disincentives for investing in privacy-protective mechanisms. This has both positive and negative implications.

As always, this edition of EDPL contains several country reports, this time about developments in Belgium, Denmark, Romania, France and the Czech Republic. Also included in the journal are two case notes written by Hielke Hijmans and Sascha van Schendel and a review of Mireille Hildebrandt's new book *Smart Technologies and the End(s) of Law*.

I hope you enjoy reading the second edition of the European Data Protection Law Review.

*Bart van der Sloot*
*Institute for Information Law,*
*University of Amsterdam*

17 <http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm>. <http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm>.<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0702&from=EN>. <http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf>.