The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember

Freedom of Expression Safeguards in a Converging Information Environment

Dr. Joris V.J van Hoboken

2013

Report EUR 26410 EN

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Ângela Guimarães Pereira
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361 , 21027 Ispra (VA), Italy
E-mail: angela.pereira@jrc.ec.europa.eu
Tel.: +39 0332 78 5340

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 86747

EUR 26410 EN
ISBN 978-92-79-35010-8

ISSN 1831-9424

doi: 10.2788/51998

Luxembourg: Publications Office of the European Union, 2013

Printed in Italy

The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember

Freedom of Expression Safeguards in a Converging Information Environment

Prepared for the European Commission Appointment Letter No. 257971 - 14 January 2013

by Dr. Joris V.J van Hoboken

Institute for Information law (IViR), University of Amsterdam, The Netherlands

Amsterdam, May 2013

Contents

1. Introduction

This report puts the EC proposal for a right to be forgotten in context and discusses it from the perspective of freedom of expression. As will become apparent, the right to be forgotten as proposed in data protection law is a concept that relates closely to the regulation of privacy harms caused by new forms of publicity online, most notably search engine and social media publicity. These new forms of publicity are the subject of daily news reports about the privacy impact of the

Internet and related services. Even though scientific literature shows that the Web is extremely volatile, that valuable information constantly disappears and that the structural preservation of historic publications online is a very hard problem, the perception that the Web never forgets seems to remain prevalent.

Acting on concerns over online publicity, over the last decade, Data Protection Authorities (in France, Spain and Italy in particular) have laid the foundation for the establishment of strengthening the control of people over the *public* data that is processed about them online through a so-called 'right to be forgotten'. The European Commission, after consulting on the topic, has made the name and (some parts of) this right into a central element of its proposal for a General Data Protection Regulation. Considering the fact that these proposals relate to new forms of publicity online, a fundamental question is whether freedom of expression is sufficiently taken into account. Much of the public debate in the general media that has taken place over the last two years about the right to be forgotten touches on this important question, that will be addressed in this report through a discussion of the proposed Article 17 and 80 and related legal doctrines. The EC proposals are discussed in detail, taking into account recent developments in the European Parliament and the Council.

The EU data protection framework seems to have become the most important legal framework for addressing privacy concerns relating to online media. This report also addresses the fundamental question to what extent this is a good development. It does so by first looking at the interface of data protection as applied to online publications of personal data and the laws at the national level relating to the lawfulness of publishing about natural persons. Second, and finally, this report looks at extremely (and ever more) complex interface of data protection with intermediary liability regulation at the EU level (limited safe harbors) and the Member States (secondary liability). Data protection law currently lacks the tools for setting the boundaries for intermediary and the current proposals do not effectively address this issue either. This raises the question of how this interface could be better established, which will be addressed in the final part of this report.

Section 2 will discuss the backgrounds of the right to be forgotten. Section 3 discusses the already existing principle and the implied right of erasure under the current Data Protection Directive. After that, the EC proposal for a right to be forgotten in Article 17 of the Regulation will be addressed (Section 4), the way data protection deals with freedom of expression concerns in Article 80 and recital 121 (Section 5) as well as some of the proposals to amend Article 17 and 80 by the European Parliament and the Council (Section 6). Section 7 discusses the interface of data protection with privacy tort law and media law and Section 8 discusses the interface with intermediary liability regulation. Section 9 concludes.

2. The Concept of the Right to be Forgotten

The concept of a right to be forgotten as such is not new. It has been explored in various specific legal contexts and under different qualifications, such as the right to have information deleted[1], the

[1] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton and Oxford: Princeton University Press 2009; C. Conley, 'The Right to Delete', *AAAI Spring Symposium Series* 2010; P.A. Bernal, 'A Right to Delete?', *European Journal of Law and Technology*, Vol. 2, No.2, 2011.

right to oblivion,[2] and social forgetfulness.[3] As will be discussed in more detail below, the characteristics and dynamics relating to publication and of information on the Internet has spurred the current debate about strengthening the right to have information deleted in the digital age.

The right to be forgotten has become a somewhat ambiguous term.[4] First, various Member States already know a right to be forgotten in their media laws as a restriction on the legality of publishing about historic events.[5] Typically, this right is only applicable in very specific contexts and restricts the legality of publishing about convicted criminals when the interest of reintegration outweighs the interests of society in being informed about the history of specific individuals and their criminal record(s). In Germany, for example, this right is informed by the interest of allowing convicted criminals to reintegrate into society; their names may not be mentioned in connection with the crime after their sentence. The right is based on a broad interpretation of the 'right to personality.'[6] Notably, this classical right to be forgotten affects the legality to publish again about historic events, such as someone's wrongdoing in the past. Typically, it does not affect the legality of historic publications themselves. In other words, these more classic doctrines do not answer the question what rules apply to making historic publications available online and allowing them to be indexed by search engines.[7]

Considerations similar to this personality right can be found in the Committee of Ministers Declaration and Recommendation on the provision of information through the media in relation to criminal proceedings.[8] In these cases, like with other restrictions on the freedom of the media to publish and inform the public about matters of public concern, a balance will have to be struck between the right to private life (Article 8 ECHR) and the right to freedom of expression (Article 10 ECHR).[9] Member States have a margin of appreciation of how to strike this balance and the balance that is struck depends on the legal culture in the Member States.

---

[2] J. Warner, 'The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps', *University of Ottawa Law & Technology Journal* Vol. 2 No. 1 (2005).

[3] J.F. Blanchette and D.G. Johnson, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness', *The Information Society* 18:1 (2002).

[4] For discussions of the right to be forgotten, see e.g. E.J. Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice', *SCRIPTed* (2011) 8:3, p. 232. J.L. Zittrain, *The Future of the Internet and How to Stop it*, New Haven & London: Yale University Press 2008, p. 228-229 as cited by J. Ausloos, 'The 'Right to be Forgotten' – Worth Remembering?', *Forthcoming Computer Law & Security Review* (2012).

[5] See e.g. A.J. Nieuwenhuis, 'Tussen verdachtmaking en vergetelheid', Mediaforum 2013/3.

[6] L. Siry and S. Schmitz, 'A Right to be Forgotten? - How Recent Developments in Germany May Affect the Internet Publishers in the US', *European Journal of Law and Technology*, vol. 3 no. 1 (2012). The Sedlmayr murderers case can be already be mentioned here. They filed lawsuits to have their names in connection with the crime they were convicted for removed, though, due to the enhanced accessibility they only challenged online archives and not traditional archives.21 Apparently, the claim regarding the German version of the Wikipedia page has been successful. However, the full names of both murderers can still be found on the related discussion page.22 Further, despite the same claim in relation to the English language version of the article, their names are still up there.23 The general counsel of the Wikimedia Foundation has stated to support both decisions of the editors.24

[7] For further discussion, see Section 8.

[8] Committee of Ministers, Declaration on the provision of information through the media in relation to criminal proceedings, adopted on 10 July 2003; Committee of Ministers, Recommendation Rec (2003) 13 on the provision of information through the media in relation to criminal proceedings.

[9] One of the appended principles to the non- binding Recommendation explicitly sees on 'Media reporting after the end of court sentences': unless there is explicit consent of persons who have served court sentences, or unless they and their prior

Second, and in the last decade, there has been discussion about a broader right to be forgotten in reaction to new forms of publicity and access to information facilitated by the Internet. There is a general unease that the Internet never forgets; the underlying idea and assumption being that the default has shifted from 'forgetting' to 'remembering'.[10] Put differently, the right to be forgotten in these discussions can be understood as a proposal to deal with new forms of publicity (or public accessibility) over time facilitated by the Internet and the Web. Thus, it can be seen as a proposal to broaden the existing right to be forgotten in media law discussed above to other practices of making information about people publicly available.

The Internet and the World Wide Web have broadened the group of individuals and organizations that can publish information and ideas.[11] It has also given rise to new services that contribute to the public information environment and facilitate access to information and ideas and provide platforms for socialization, discussion and debate. Search engines have a particular role in these discussions of course, since they help users to retrieve information about individuals posted online, regardless whether it is still relevant, correct, or favorable for the particular individuals involved. It is well-understood that indexation of the online environment by search media can adversely affect people's privacy or reputation, but typically search media are not considered liable for the content of others on the basis of specific exceptions (or safe harbors) at the European and national level.[12] Social media and other platforms facilitating online interaction between people, such as news groups, discussion forums and comment sections also play an important role in these discussions.[13] Interactions on social media often take place in public or semi-public places that do not effectively restrict the further proliferation and future findability of the information involved.

While the sentiment that the internet never forgets is widespread, it is indeed a 'sentiment', and in general quite incorrect. There may be some cases of publicity about people that will indeed never be forgotten and of course, it may be true that for all of us there is something that remains online. The best examples of the things that will never be forgotten are of course the memes relating to natural persons such as the 'Star Wars Kid' or the 'Dog Poop Girl', or to public figure that experience the so-called Streisand Effect,[14] a good example of which is the Max Mosley.[15] These cases are remarkable but rare, however, and the Streisand Effect demonstrates that it is questionable how much the law can do to prevent them.

---

offence are of public concern again, their identity in connection with their prior offence should be protected under Article 8 ECHR in order to enable reintegration into society. See CM/Rec (2003) 13, Principle 18 and CM/Rec (2003) 13, Explanatory Memorandum, point 40.

[10] Mayer-Schönberger 2009, p. 2. See also A.W. Hins, 'Het ijzeren geheugen van internet', Ars Aequi 2008-07/08, p. 558. P.S. Castellano, 'The right to be forgotten under European Law: a Constitutional debate', Lex Electronica vol. 16.1 (Hiver/Winter 2012), p. 4.

[11] See Joris van Hoboken, *Search engine freedom. On the implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*, Information Law Series 27, Alphen aan den Rijn: Kluwer Law International 2012.

[12] For a discussion, see Section 8. See also Van Hoboken 2012. Many of the insights in this report are derived from this book which was the result of a PhD research project at the Institute for Information Law at the University of Amsterdam from 2006-2011.

[13] For a discussion of the dynamics resulting from online media on reputation, see Daniel Solove, *The Future of Reputation*, New Haven & London: Yale University Press, 2007.

[14] See Wikipedia, Streisand Effect, http://en.wikipedia.org/wiki/Streisand_effect.

[15] For a discussion, see supra note 13.

The information preservation sector, i.e. (digital) archives and libraries, has consistently voiced its concerns about the highly ephemeral nature of the internet. More than a decade ago, the lifespan of webpages was estimated between 75 and 100 days. Consequently, material of possible historical value and thus an important part of the public information environment was argued to "vanish with disturbing speed."[16] More recently, the communities engaged in developing methods for Web preservation and those studying the capacity of the Web to remember do not sound less alarming. In an article gloomily titled 'Avoiding the Digital Dark Age', Bollacker describes the problems of keeping a record of digital data, which are manifold.[17] The 'Digital Dark Age' refers to the idea that

> "the pace of adoption of new digital technologies can outstrip the development of the infrastructure required for sustainable access to its outputs, ultimately leading to the loss of data."[18]

A review of the literature teaches that not only the practices surrounding 'forgetting', but precisely those related to remembering and the preservation of information and a historical record are undergoing and need to undergo radical change and warrant careful attention by policy makers.[19]

Some have argued in favor of the right to be forgotten as a 'clean slate approach'. For instance, in the context of the possibility of a fresh start on the internet, Jonathan Zittrain proposed the concept of "reputation bankruptcy", modeling his proposal on a sector-specific data protection in the US, called the Fair Credit Reporting Act.[20] It must be noted here that, because of the dominance of U.S. authors in the discussion about the right to be forgotten, references to the U.S. discussion about possible legal proposals can have some problems and can take some work to be put into a European context.[21] The legal regime as regard data protection, online privacy and reputational infringements

---

[16] N.O. Finneman, 'Internet – a cultural heritage of our time', *Conference Proceedings: Preserving the Present for the Future*, Danish National Library Authority/Denmark's Electronic Research Library, Copenhagen 2001, p. 32.

[17] Kurt D. Bollacker, 'Avoiding a Digital Dark Age', American Scientist, 2010.

[18] See Stuart Jeffrey, 'A new Digital Dark Age? Collaborative web tools, social media and long-term preservation', World Archaeology, Volume 44, Issue 4, 2012.

[19] See e.g. Hany M. SalahEldeen, Michael L. Nelson, 'Losing My Revolution: How Many Resources Shared on Social Media Have Been Lost', Theroy and Practice of Digital Libraries, 2012 (concluding that 27% of social media content was lost after just a few years); Ziv BarYossef et al., 'Sic Transit Gloria Telae: Towards an Understanding of the Web's Decay', WWW2004, 17-22 May, 2004, New York, USA, ACM 158113844X/04/0005 ("In addition to just individual pages, collections of pages or even entire neighborhoods of the web exhibit significant decay, rendering them less effective as information resources."); Privacy Implications of Digital Preservation, 3 Elon Law Review 133, 2011-2012 (calling on the government to take its responsibility for modernizing memory institution activities for the digital age); Frank Crown et al., 'Why web sites are lost (and how they're sometimes found)', Communications of the ACM, Volume 52 Issue 11, November 2009 (concluding that many websites that do disappear can not be found in existing Web repositories); Marieke Guy, Alexander Ball, Michael Day, 'Missing Links: The Enduring Web', International Journal of Digital Curation, Vol. 4, No. 2, 2009, p. 135-143 (asking "How can we carve a legacy from such complexity and volatility?"); Viveca Asproth, 'Information Technology Challenges for Long-term Preservation of Electronic Information', International Journal of Public Information Systems, vol. 2005, nr. 1; Michael L. Nelson, 'A Plan For Curating "Obsolete Data or Resources"', Position paper for the UNC/NSF Workshop "Curating for Quality: Ensuring Data Quality to Enable New Science", 10-11 September 2012 (concluding that "unfortunately, the technology for publishing information on the web always outstrips our technology for preservation."); Richard Davis, 'Moving Targets: Web Preservation and Reference Management', Innovations in Reference Management workshop, January 2010; Edgar Crook, 'Web archiving in a Web 2.0 world', The Electronic Library, Vol. 2, nr.: 5, p.831 – 836, 2009.

[20] For a discussion, see Jeffrey Rosen, The Web Means the End of Forgetting, NY Times, 21 July 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

[21] Recent contributions include Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88, 2012; CDT, On the Right to Be Forgotten: Challenges and Suggested Changes to the Data Protection Regulation, 2 May 2013.

is really different in the U.S. Hence they start from a totally different background and legal reality. There is no general data protection law in the United States and for public data, the First Amendment weighs heavily. Furthermore, the U.S. legislature passed a law in 1996, the Communications Decency Act, that legally protect intermediaries from all liability for the postings of third parties (CDA, Section 230). This has resulted in some rather extreme cases of harmful content remaining online without a clear possibility for data subjects to address them.[22]

Koops distinguishes two 'clean-slate' perspectives as discussed in scholarly literature, namely the 'social' variant in which people should not be confronted with "outdated negative information" and the 'individual' self-development alternative that focuses on the right to forget, which allows people to act freely without being restrained by "fear for future consequences."[23] It is important to note here that there is also a more relaxed variant possible, namely that restrictions are placed on the legality of using certain old information against someone without proper safeguards in place (such as transparency). And while people may not realize this is the case, EU data protection laws already has entails a regime for the systematic use of online resources, which for instance covers the online screening of candidates though a search for available online data by employers in the job application process. Outside personal and household use, to access and use personal data accessible online one needs a legitimate purpose that data subjects should be informed about.

In the context of the Council of Europe, several references to the right to be forgotten can be found going back to the end of the 1980s. In 1989, the Council of Europe's Committee of experts on data protection (CJ-PD) mentioned 'the right to be forgotten' in the context of data obtained through telemetry, that should be "erased after a certain time."[24] Another reference to the right to be forgotten can be found in a CoE CJ-PD report from 1990. This report criticizes the right of the data subject to "rectify erroneous reports which are stored in electronic [media] archives, with the danger that in so doing history may be rewritten?"[25]

Third and finally, there is a 'right to be forgotten' as proposed by the European Commission as part of the new Data Protection Regulation. On the one hand, this proposal logically builds on the general (and already existing) obligation of data controllers to stop processing (thus delete, since storage is processing too) personal data when a legitimate ground and purpose for their processing no longer exists. The European Commission proposal strengthens this existing obligation by stipulating an actual right in Article 17 of the Regulation to have one's data deleted in situations in which their processing is no longer legitimate, for instance if the processing was based on consent and such consent has been withdrawn. Thus, this 'right to be forgotten and erasure' can be seen as a mirroring provision for the existing provision on legitimate ground for processing in Article 7 of the current Data Protection Directive (DPD). More generally, the European Commission has positions this right to

[22] For a discussion, see e.g. Brian Leiter, 'Cleaning Cyber-Cesspools: Google and Free Speech', in: Saul Levmore, Martha C. Nussbaum (eds.), The Offensive Internet, Harvard University Press, 2011, Kindle Edition. Fo a discussion, see Van Hoboken 2012.

[23] Koops 2011, p. 234.

[24] Committee of experts on data protection (CJ-PD), 'New technologies: a challenge to privacy protection?' study prepared under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1989, p. 11.

[25] Committee of experts on data protection (CJ-PD), 'Data protection and the media', study prepared under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1990, point 11.

have one's data deleted as one of the ways to strengthen the individual's control over its personal data.

On the other hand, however, the European Commission proposal (article 17, second paragraph), and the arguments that have been put forward for it, contain elements that specifically relate to public information and new forms of publicity facilitated by the Internet discussed above. It is this second nature of the proposed right to be forgotten in the Regulation that has given rise to much of the debate about the possible negative impact on the right to freedom of expression. This debate and the possible ways to address the issues that have been put forward will be discussed in more depth below.

In both situations the idea under data protection would be that data would have to be deleted in due time. In other words, under data protection law, the right to be forgotten presupposes that the processing has been legal for a certain period of time, after which the data would have to be deleted. This is an important distinction with respect to laws that determine whether a certain processing operation was legal in the first place. A second point of note is against whom the right could be invoked. Like other data subject rights, the right to be forgotten can be invoked against the data controller. Considering the debates about the question of who can be considered the controller (as defined under data protection law) in the context of online publications, references, and copying, of personal data, this aspect could lead to some very difficult interpretation issues. This is especially of concern since the arguments for the proposal often feature examples of personal data on social networks or in search engines. It is not precisely clear whether such intermediaries can and should be considered controllers as regards the personal data posted by third parties.[26] In addition, there are complicating questions of whether an individual can be seen as a controller too.[27]

3 The Existing Right to Erasure under the current Directive (DPD)

Under current data protection rules, Directive 95/46/EC, there is an implied right of having one's data erased if the processing (including storage) is no longer lawful. And a more explicit right follows from Article 12(b) DPD, which focuses in particular on the situation of incomplete or inaccurate data. In general, a right to erasure, however, follows from the purpose limitation principle in Article 6 DPD in combination with the need for a legitimate ground in Article 7 DPD. Personal data may only be collected for specified, explicit and legitimate purposes and at least one of the legitimate grounds for processing of data must apply. In relations between private actors, such as an online services and their users or third party data subjects, the processing of personal data will typically be based on Article 7(a), (b) or (f) DPD, i.e. there is unambiguous consent for the processing, and/or it is necessary for the performance of a contract and/or it is necessary on the basis of the legitimate interests of the controller or a third party and these are not overridden by the interests of the data subject.

In cases in which the processing is based on Article 7(e) or (f) DPD, there is also a specific data subject right to object in Article 14 DPD. In order to successfully invoke this right, the data subject must show specific circumstances that constitute "compelling legitimate grounds." When an objection is

[26] See Section 8.

[27] Koops 2011, p. 238-240. See on the issue of individuals as controllers also Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010; N. Helberger and J.V.J. van Hoboken, 'Little Brother Is Tagging You - Legal and Policy Implications of Amateur Data Controllers', *Computer Law International (CRi)*, 2010-4.

justified, the data may no longer be processed. Notably, there is no duty to inform data subjects on which legitimate ground the processing is based, which means that data subjects will not always be aware of the right to object outside cases of direct marketing. More specifically, the processing of personal data in relation to online services is often only partly based on the consent of the data subject (or the performance of the contract), which means that the mere termination of the service will not trigger an obligation to stop processing data. Furthermore, it has become industry practice to formulate very open-ended purposes for processing, thereby making it easier to defend the continuous processing of persona data of data subjects under such purposes.[28] And finally, while the processing of certain specific data may at some point no longer be necessary for one purpose, there may be other purposes for which the processing of this data is still needed, legitimate and lawful.

While these principles and general rules are clear, in practice, the application of these rules can get cumbersome and tends to lead to complicated end results.[29] In this regard, the clarification of obligations and data subject rights would be very valuable. The complexity resulting from the application of current rules, which is unfortunately not really addressed by the GDPR, can be shown by a short example of a social networking service. Note that a data subject is an 'identified' or 'identifiable' person to whom certain data relate (Article 2(a) Data Protection Directive). The controller is the person or entity that determines the purposes and means of the data processing (Article 2(d) Data Protection Directive).

In case of social networking sites, a processing operation (of semi-public personal data) would typically involve the platform as well as other users. Hence, the data subject would probably have to deal with both categories of controllers in some way when seeking compliance with data protection rules.[30] In practice, the responsibility for data processing will be distributed between the social network provider and other users and it is likely that in practice the controllers involved could try to escape responsibility by pointing to the other.[31] For instance, other users can decide to post pictures of others online, tag them and make them available for unlimited audiences. Would they want to take the full responsibility for being able to reach a world-wide audience with an unlawful publication of personal data? The complexity increases even more since there are multiple legitimate grounds that could be invoked by the applicable data controllers for various data processing purposes. Some of the data processing will be necessary for the delivery of the service, such as the registration on the site and the making the data available to others. For other data processing purposes, additional consent of the data subject could be required, but there are also data processing purposes, for instance for the security of the site for which no consent is needed from the data subject in the first place.

To go back to the existing rules with regard to erasure, the existing framework does contain an implied duty to stop processing personal data if the processing no longer fulfills a legitimate purpose. Hence, data controllers already have a duty to erase data that are no longer needed for legitimate purposes as the processing would not be lawful anymore.[32] Thus, the determination of when data

[28] See for instance the exchange between Google and CNIL about the change to Google's privacy policy. Google has formulated one very broad purpose for all the data that it collects (and combines).

[29] See also Section 7 and 8.

[30] Helberger and Van Hoboken 2010, supra note 10, p. 102.

[31] See Article 29 Working Party, 'Opinion 5/2009 on Online Social Networking', 12 June 2009.

[32] See Bernal 2011, supra note 1.

would really need to be deleted is very complex in practice. Since this complexity is caused by the application of the basic definitions and rules relating to controller, purpose limitation and legitimate ground, this complexity is likely to stay after the passing of the GDPR.

The role of certain national Data Protection Authorities (DPAs) in shaping the proposal for a right to be forgotten as a way to address online publicity issues seems to have been significant. Italian, Spanish and French DPA´s have explicitly recognised 'il diritto all'oblio', 'el derecho al olvido' and 'le droit à l'oubli'. [33] In Italy, the right to be forgotten was already shortly mentioned in a case before the Italian Supreme Court in 1998 relating to the press and it has been referred to in the data protection context later on by the Italian DPA (Garante).[34] Garante grounds this right on the data quality principle and in this context emphasizes the character of the internet, on which information can easily be found with search engines. Thus, Garante clearly situates the right as a way to address possible harm following from public information and new forms of publicity online, more than a general data protection principle that data should not be processed longer than necessary. According to Garante, after a certain time and when the data has served the purpose for which it was processed, there must be possibilities to delete data as otherwise legitimate rights may be affected.[35]

The Spanish DPA (AEPD) has been particularly active as regards the right to be forgotten as related to the online environment. It has ordered search engines to de-index links to old information published online elsewhere.[36] This has led to legal action between the AEPD and Google Spain that is currently pending at the CJEU.[37] The AEPD has identified the capacity of the individual involved and the newsworthiness of the event as relevant criteria for the application of a right to be forgotten in relation to search engines: a citizen who is neither a public personality, nor subject of a news event of public relevance must enjoy corrective mechanisms to "turn public information into private information at a certain time by no longer allowing third parties to access such information."[38] However, not only has the AEPD ordered Google to delete links to inaccurate or outdated information, apparently it considers the right to object to be applicable to the processing of lawfully public information indexed by search engines as well, such as newspaper articles or official government publications online. [39]

---

[33] See Castellano 2012, supra note 10.

[34] Italian Supreme Court 9 April 1998, no. 3679.

[35] Castellano 2012, supra note 10, p. 21. See also L. Liguori and F. De Santis, 'The "right to be forgotten": privacy and online news', MediaLaws, 18 March 2011.

[36] See See AEPD, Statement on Internet Search Engines 12, 1 December 2007 ("[t]he AEPD has been defining, via a number of decisions, criteria for protecting the right of cancellation of the information available on the Internet and, specifically, the appropriateness of the right of opposition in respect of search engine services"). Don X.X.X. v. Google Spain, S.L., AEPD Res. no. R/01046/2007, Proc. no. TD/00463/2007 (Nov. 20, 2007), dealing with a request of removal from Google's search results by a natural person results in the following administrative order: "calling on Google to adopt the necessary measures to withdraw the data from its index and block future access to it." (id., at 10). This is not only noteworthy because the obligation of removal is based on data protection legislation, but also because the source of the information, a publication of personal data by local Spanish authorities, is considered to be lawful. Of note as well, is that both these official publications are no longer available online at the location at which they were published.

[37] See also Van Hoboken 2012, Van Hoboken 2008. For further discussion, see also Section 4.1.

[38] See Castellano 2012, supra note 10, p. 11-12.

[39] Castellano 2012, supra note 10, p. 13-14.

Not surprisingly, the demand of AEPD that Google deletes – even lawfully published - content from its indexes is not without critique. Considering the importance of search engines for the online environment, the rule could threaten to make search engines an indirect tool of censorship.[40] Recently, the Spanish National Court has issued a decision in a case that involves Google. Yet, no statements were made about the scope and conditions of the right to be forgotten: the case was dismissed due to Google Spain's "lack of standing to be sued."[41] As mentioned above, the Spanish Court addressing the case between Google and AEPD has asked for guidance by asking preliminary questions to the European Court of Justice.[42] With the question concerning the right to be forgotten, the court essentially asks whether an individual can prevent search engines from indexing personal information on the basis of the existing rights to erasure (Article 12(b) General Directive) and to object (Article 14(a) General Directive), even when the content was legally published.[43] The interpretation of the European Court of Justice could be important both for the scope of the rights under current data protection law and for the proposed right to be forgotten, although the question sees on the latter right in the specific context of search engines and not on the right in general. The fact that these rules are also being reviewed and debated in the context of the GDPR is of course complicating matters.

In France, the notion of a 'right to be forgotten' is said to have served as the basis for the data minimization principle for decades.[44] Indeed, the French DPA (CNIL) has recognized the right to be forgotten in relation to data protection principles in an early stage. For example, the right was placed in the context of the networked environment, and later on the scope of application was extended to the online world.[45] For according to CNIL, the right to be forgotten is of special importance on the Internet. The premise is that the continued availability of personal data on the internet poses threats to the individual's freedom of expression and the freedom to change his opinions. Therefore, CNIL welcomed the renewed debate in France on the topic.[46] Furthermore, it stated to be in favor of the French legislative proposal that was issued in 2009.[47] This intended to strengthen the right to be

[40] See supra note 11.

[41] M. Peguera, 'Google Spain wins lawsuit over the "right to be forgotten"', 27 February 2012, available at: http://ispliability.wordpress.com/2012/02/27/google-spain-wins-lawsuit-over-the-right-to-be-forgotten/; M. Peguera, 'More on the Alfacs v Google case and the "right to be forgotten"', 29 February 2012, available at: http://ispliability.wordpress.com/2012/02/29/more-on-the-alfacs-v-google-case-an-the-right-to-be-forgotten/.

[42] See CJEU (Reference), Google v. Spain, C-131/12. For a discussion of the public hearing in this case, see Ausloos, 'Google v Spain at the European Court of Justice', 5 March 2013, http://jefausloos.wordpress.com/. The AG opinion is scheduled for 25 June 2013.

[43] M. Peguera, 'Spain asks the ECJ whether Google must delete links to personal data', 2 March 2012, available at: http://ispliability.wordpress.com/2012/03/02/spanish-court-asks-the-ecj-whether-google-must-delete-links-to-personal-data/. See also P. Fleischer, '"The right to be Forgotten", seen from Spain', 5 September 2011, available at: http://peterfleischer.blogspot.com/2011/09/right-to-be-forgotten-seen-from-spain.html.

[44] J.F. Blanchette, 'Not Just Left Alone, But Forgotten Too! The Case of French Law', Proceedings of the American Society for Information Science and Technology, Vol. 43, issue 1 (2006).

[45] Castellano points at Commission Nationale de L'Information et des Libertés (CNIL), 20ème Rapport d'Activité 1999', available at: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//004001043/0000.pdf.

[46] Commission Nationale de L'Information et des Libertés (CNIL), '30ème Rapport d'Activité 2009', p. 29, available at: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf. See also Y. Padova, 'Pas de liberté sans droit à l'oubli dans la société numérique', 27 November 2009, available at: http://www.cnil.fr/la-cnil/actualite/article/article/pas-de-liberte-sans-droit-a-loubli-dans-la-societe-numerique/.

[47] Id.

forgotten in the digital environment.[48] Despite the fact that the proposal has not become law yet and the current legislation consequently does not contain an explicit right to be forgotten, symptoms of such a right are already visible in French case law.[49] In the same sense, when the right to be forgotten appeared for the first time on the European Commission's policy agenda, the French DPA indicated to be in favor of the forthcoming legislative proposal on the right to be forgotten.[50] Next to these legislative initiatives, the French Secretary of State and Prospective Development of the Digital Economy initiated a 'Code of Good Practice on the Right to Be Forgotten on Social Networks and Search Engines'. The Code was signed in 2010 and aims to enhance user control over their digital data.[51]

Considering the featuring of search engines in these discussions in Spain, France and Italy, it is worth noting that there is no reference to a 'right to be forgotten' in the Article 29 Working Party opinion on search engines that was adopted in 2008.[52] This would have been a logical place to come to an agreement on the issue. Article 29 does recognize the impact of search results on individuals concerned:

> "The representation and aggregation capabilities of search engines can significantly affect individuals, both in their personal lives and within society, especially if the personal data in the search results are incorrect, incomplete or excessive."[53]

However, as regards to the question whether search engines should have to remove personal data from their index or search results, the opinion signals divergent approaches in the member stats:

> "the extent to which an obligation to remove or block personal data exists, may depend on the general tort law and liability regulations of the particular Member State."[54]

The Article 29 Working Party also signals that the law should be careful not to consider search engines as the primary controller for the personal data in their index.[55] More generally, it clarifies that:

> "A balance needs to be struck by Community data protection law and the laws of the various Member States between the protection of the right to private life and the protection of personal

[48] M.Y. Détraigne and A.M. Escoffier, 'Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique', 6 November 2009, available at: http://www.senat.fr/leg/ppl09-093.html.

[49] Apparently, the proposal has thus far not yet been approved. See the overview of Naftalski and Desgens-Pasanau. They state that the notion of a right to be forgotten is not formally contained in the French Data Protection Act of 1978. F. Naftalski and G. Desgens-Pasanau, 'Projet de règlement européen sur la protection des données: ce qui va changer pour les professionels', *Revue Lamy Droit de l'Immatériel*, March 2012, no. 8, p. 71. See also the press release on legalis.net, 'Droit à l'oubli: Google contraint à la désindexation', 19 March 2012.

[50] Commission Nationale de L'Informatique et des Libertés (CNIL), '31e Rapport d'Activité 2010', p. 38, available at: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_rapport_annuel_%202010.pdf.

[51] 'Code of Good Practice on the Right to Be Forgotten on Social Networks and Search Engines', http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf

[52] Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines, Brussels, 4 April 2008.

[53] Id.

[54] Id.

[55] Id.

data on the one hand and the free flow of information and the fundamental right to freedom of expression on the other hand."[56]

We will come back to these considerations in Section 8.

4. The Proposal for a Right to be Forgotten by the European Commission

The European Commission proposal for a new General Data Protection Regulation aims to modernize the current data protection framework in order to meet new challenges to data protection posed by enhanced data sharing and collecting. The GDPR contains a number of new elements, but it also reflects the European Commission's view that the underlying principles and objectives of the current Directive remain valid.[57]

Looking at the various European Commission documents and speeches by Commissioner Reding, the right to be forgotten plays the role of meeting one of the main challenges identified by the Commission, in particular the need to give data subjects more control over their data.[58] In 2010, the EC already considered "the so-called right to be forgotten, i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."[59] Ever since, the right to be forgotten has become a central element in the EC proposals and the debates about it by policy makers, academics and the general media. [60] So in that regard, the right to be forgotten has been a major political success.

The general objective of the European Commission is to strengthen the rights of individuals to protect their personal data. It is of the opinion that personal data can easily be stored and multiplied on the internet, while at the same time "it is not easy to wipe [them] out."[61] The right is especially mentioned in the context of search and social media. Other context factors that are mentioned are the opportunities for "unlimited search and storage".[62] On later occasions Commissioner Reding has reiterated the focus on ensuring that "privacy rights are put into action" and increased user control.[63]

---

[56] Id.

[57] EC, 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 final, 2012/0011 (COD), Brussels, 25 January 2012.

[58] For backgrounds, see Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', Brussels, 4 November 2010, Com(2010) 609. The EC's Communication and the consultation replies can be found here: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

[59] Id., p. 8.

[60] See *infra* note 60-66 and accompanying text.

[61] See for an explanation of the reform plans: V. Reding, 'Privacy matters – Why the EU needs new personal data protection rules', Brussels, 30 November 2010.

[62] Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, 'The future of data protection and transatlantic cooperation', Speech at the 2nd Annual European Data Protection and Privacy Conference Brussels, 6 December 2011.

[63] Viviane Reding, Vice-President of the European Commission EU Justice Commissioner, 'Your data, your rights: Safeguarding your privacy in a connected world', Privacy Platform "The Review of the EU Data Protection Framework" Brussels, 16 March 2011.

More specifically the right to be forgotten is presented as part of a "comprehensive set of existing and new rules to better cope with privacy risks online."[64] Commisioner Reding emphasises the fact that people should have the right, "and not only the possibility", to withdraw consent to data processing. In this regard, data processors have to prove that they need to keep processing the data.[65] Already in 2011, the European Commission acknowledged that the right to be forgotten is also a "difficult issue."[66] Soon after the actual proposal for the GDPR had been published, Commissioner Reding also explicitly addressed the relationship with freedom of expression and clarified the right to be forgotten is not absolute and "cannot amount to a right of the total erasure of history."[67]

In the EC proposal for the GDPR, Article 17 contains the actual right to be forgotten and erasure. Article 17(1) stipulates the situations in which such a right can be invoked. Article 17(2) contains an additional obligation in cases in which the data has been made public. Article 17(3) provides for some exceptions. Article 17(4), (5) and (6) stipulate a number of situations in which the data do not have to be erased but their processing should be restricted. Article 17(7) and (8) contain an obligation to implement time limits for the storage and erasure of data and an obligation not to otherwise process data after erasure. Article 17(9) provides for the possibility to adopt delegated acts for the European Commission.

> **Article 17 Right to be Forgotten and to Erasure**
>
> 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
>
> (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
>
> (c) the data subject objects to the processing of personal data pursuant to Article 19;
>
> (d) the processing of the data does not comply with this Regulation for other reasons.
>
> 2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal

[64] Id.

[65] Id. See also Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age', Innovation Conference Digital, Life, Design Munich, 22 January 2012.

[66] V. Reding, 'Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age', Brussels, 7 December 2011.

[67] Supra note 63.

> data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

In the following, the discussion will be restricted to the most important elements of Article 17 for the purposes of this paper, namely the first and second paragraph cited below. As has been noted by others, the exceptions in Article 17(3) may be superfluous. For instance, the obligation ex Article 17(3)(a) to take the right to freedom of expression into account in accordance with Article 80, also seems to follow from Article 80 itself.[68] Article 17(4) deserves some mention here to the extent that it suffices to merely contest the accuracy of data. Consequently an obligation to restrict processing would arise, even without it being necessary to give some evidence that the data are incorrect. This could possibly lead to situations of abuse to have data online become inaccessible. Apparently, Article 17(9)(b) still refers the text of Article 17 (2) from an earlier version of the EC proposal. It refers to "the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2", but no such services are referred to in Article 17(2) of the proposal.

Article 17 (1) combines elements from both Article 12 and Article 14 of the General Directive. First, it confers on the data subject a right to erasure of personal data, which also follows from Article 12 General Directive. Second, data subjects shall have the right to obtain from the controller the abstention from further dissemination of personal data, which resembles the right to object to further processing as contained in Article 14 of General Directive. Article 17 (1) of the proposal then goes on to list the grounds on which these rights can be invoked: if the data are no longer necessary in relation to their original purposes (a), if the data subject withdraws consent or the storage period which it consented to has expired (b), if the data subject objects to the processing of personal data (c), or if there are other reasons why the processing does not comply with the provisions of the Regulation (d). In sum, when there is no longer a legal basis for the processing.

According to the Commission, Article 17 "further elaborates and specifies" the rights contained in Article 12(b) General Directive. However, based on the above, the added value of Article 17(1) for data subjects that want to see data deleted is by itself relatively minor.[69]

Generally speaking, the impact of Article 17 will strongly depend on the question of whether GDPR will help to establish a more strict interpretation of the purpose limitation principle by data controllers in combination with a strict interpretation of legitimate ground, and not (only) on the adoption of Article 17 itself. Notably, the EC proposal does contain a number of elements that amount to the strengthening of purpose limitation.[70] For instance, it contains an obligation to inform data subjects of the period for which data will be processed, which is also reflected in Article 17(1). However, the GDPR does not stipulate in what way these periods need to be defined by data

[68] See e.g. European Data Protection Supervisor 2012, par. 149. Notably, the wording in Article 17(3)(a) is hard to interpret in connection with Article 80. Article 80 does not really give meaning to the exception, but merely instructs the member states to do something. So how one could exercise the right to freedom of expression "in accordance with" Article 80 is unclear.

[69] See also Joris van Hoboken, 'Het recht op vergetelheid: een oud recht in een verkeerd jasje', Column, Privacy & Informatie, 2012-3, p. 126-127.

[70] As discussed under Section 5 however, there is a lot of pressure on weakening general definitions and principles, which could really impact on the ability of data subjects to exercise control over data relating to them, used to make decisions affecting them, and shaping the world around them.

controllers and there is nothing in the proposals that prevents the controller from defining the period in a vague manner. Article 28(2)(g) requires that data controllers make a "general indication of the time limits for erasure of different categories of personal data". The criteria ´as soon as technically possible and no later than 1 month after the data are no longer necessary for purpose X´ would seemingly suffice to comply with this rule. Recital 30 states that "the period for which the data are stored is limited to a strict minimum". The use of the word minimum instead of maximum is peculiar considering the fact that the idea would be to have data deleted as soon as possible.

Article 17(2) can be considered more revolutionary even though the text of the actual EC proposal is ambiguous and possibly inconsequential.[71] The connection to online publicity is still present, however, and by specifically referring to public information, it contains an important difference with the current Directive, which does not contain specific data subject rights in relation to public information.[72] As will be discussed in more detail below, the adoption and application of specific data protection rules to public information presents some clear issues with regard to the balancing with freedom of expression and raises the question of how Article 17 relates to Article 80 and underlying case law of the CJEU (*Satamedia*).[73]

Notably, Article 17(2) does not contain an obligation to erase or stop processing data, but only an obligation to inform others that the data subject has requested deletion. It requires that the data controller who has made the data public "shall take all reasonable steps (...) to inform third parties which are processing such data" of the erasure request. The EDPS has stated that Article 17(2) thus contains an obligation of endeavor instead of an obligation of result and considers this "more realistic from a practical point of view".[74] When reading the provision carefully, this conclusion does not seem to be correct. Actually, the provision is an obligation of result, but not with regard to the deletion of data, but with regard to the informing of third parties that have also published the personal data (and were also authorized to do so).

The obligation to inform in Article 17(2), however, is only applicable in cases which the controller can be considered "responsible" for a third party publication, which is the case if it "has authorised" this third party's publication of personal data. Since Article 17(2) only applies to data that have been made public, this restriction is surprising. In cases of data that have been made public, there is no practical need to acquire authorization to be able to publish (or use) these data elsewhere. Although it will depend on the way in which the further undefined notion of authorization would be applied in practice, it is quite possible that Article 17(2), if adopted in its current form, would only seldom apply. Considering all these issues with the wording, it is rather unpredictable how Article 17(2) as proposed by the EC will be interpreted in practice and whether it will have any real impact.[75]

Since the text of the proposal is so ambiguous and some of the earlier EC proposals were widely discussed in the media, it is worth looking at the background to earlier versions of the proposal

[71] This is especially true for the more far reaching version of Article 17(2) in the widely discussed leaked draft proposal in December 2011.

[72] It does contain some *exceptions* for public information, e.g. in Article 8(e), 18(3), 21, 26(1)(f).

[73] See CJEU 16 December 2008, C-73/07 (*Satamedia*). For a discussion, see e.g. Wouter Hins, De journalistieke exceptie en de bescherming van persoonsgegevens, Mediaforum 2013-4.

[74] European Data Protection Supervisor 2012, section 147.

[75] As will be discussed in Section 6, it is likely that the wording of Article 17(2) will change significantly.

shortly. The corresponding Article 15(2) in version 56 of the European Commission, contained the following language:

> 2. Where the controller referred to in paragraph 1 has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data.[76]

Article 17(2) GDPR no longer contains this reference to publicly available communication services which allows or facilitates the search or access to information. As a consequence, it is now (perhaps even more) unclear what contexts and situations Article 17(2) applies to.[77] In addition, the draft Article 15(2) above also contained an obligation on the source of information published online to get it removed elsewhere, which could be considered particularly problematic.[78] The fact that the controller would have been made responsible for ensuring the deletion of information elsewhere seems indeed unreasonable.

Notably, an even earlier draft of the European Commission contained a provision that merely stipulated that after information had been deleted online, the data subject also would have a right to have references to such information deleted as well.

> 2. The data subject shall have the right the right to obtain the erasure of any reference to data, which are erased pursuant to paragraph 1, from any publicly available communication service which allows or facilitates the search of or access to this data.[79]

Compared to this provision from version 51, which seems clear and unproblematic and does contain a real right for data subjects, the information obligation in Article 17(2) as proposed is ambiguous. The foregoing also makes clear that the proposed Article 17(2) does not help to establish a 'true' right to be forgotten, as some may think is still the case.

In sum, it seems fair to conclude that where the Commission apparently wanted to clarify and somewhat strengthen data subjects rights in the online environment, there are many aspects of Article 17 as proposal by the Commission that would need amendment and clarification to achieve this goal. Moreover, the added value of Article 17 compared to the existing rules seems to mostly relate to information made public, but when reading the current text as proposed by the Commission a mere obligation to inform authorized third parties remains.

As regards the impact of Article 17 on freedom of expression, which will be discussed further in the next sections, this will also depend on the interpretation of Article 17(1) in combination with Article 80. As the discussion of the media exception will show, the fundamental question rises whether a right to have information deleted should be applicable to information that is meant to inform the public. More generally, the question is to what extent the media exemption will shield certain

[76] http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf

[77] Due to the use of broad terms such as "search and access" and "allows or facilitates" the potential scope was already significantly broad.

[78] For a critical discussion, see Joris van Hoboken, "9 Reasons Why a 'Right to Be Forgotten' Is Really Wrong," jorisvanhoboken.nl, blog post, 8 December 2011.

[79] EC Proposal, draft version 51, on file with the author.

intermediaries that the right to be forgotten has been particularly been aimed at, such as search engines and social media.

Looking at reports about the proposal for a right to be forgotten, it may have been somewhat confusing for the general audience. Consider for instance Dutch newspaper reports about the reform proposals by stressing the right to be forgotten under headlines such as "*EU-burgers mogen info op internet schrappen*" (EU citizens may remove information from internet)[80] and "*EU-burgers krijgen recht om online data te laten verwijderen*"[81] (EU-citizens obtain the right to have online data deleted). By now, the public may have different expectations from the right to be forgotten than what the current proposals actually entail. This negatively affects the relation and trust people have with and in privacy regulation, which seems a negative political end-result that could outweigh the attention to data protection that the right to be forgotten succeeded to establish.

5. Public Information, Data Protection and the 'Media Exception'

To discuss the way in which a right to be forgotten as proposed in the GDPR could interfere with freedom of expression online, it is important to discuss the way in which data protection law has dealt with the possibility that some of its rules may be incompatible with freedom of expression as protected in Article 10 ECHR, Article 11 EU Charter and in the Constitutions of the Members States. Generally, the European Commission recognizes that data protection may affect other fundamental rights, amongst which the right to freedom of expression.[82] To reconcile these fundamental rights, a balance has to be found and this balance may depend on the different national cultural traditions.[83]

The principle ways in which data protection is reconciled with the right to freedom of expression is the so-called 'media exception'. While the idea behind this exception is clear, the discussion will show that both the scope and implications of this exception are unclear, and consequently the applicability of proposed Article 17 (as well as other obligations potentially restricting freedom of expression) as well. The unclear scope and implication of Article 80 is particularly concerning considering newly proposed rights to have information deleted, the increased fines that can be imposed by DPAs and the unclear status of internet users, and various types of intermediaries such as search engines, social networks, and other new media under data protection rules.

Currently, Under Article 9 of Directive 95/46, Member States must introduce exceptions for the processing of personal data "carried out solely for journalistic purposes or the purpose of artistic or literary expression, only if they are necessary to reconcile the right to *privacy* with the rules governing freedom of expression" (emphasis added). This provision remains the basis for the newly

[80] See the ANP press release that appeared in various newspapers on 26 January 2012 in the Netherlands, for instance de Volkskrant, EU-burgers mogen informatie van internet laten verwijderen, 25 January 2011, http://www.volkskrant.nl/vk/nl/2694/Internet-Media/article/detail/3137682/2012/01/25/EU-burgers-mogen-informatie-van-internet-laten-verwijderen.dhtml.

[81] See the news item on www.nu.nl, 25 January 2012: http://www.nu.nl/internet/2723895/eu-burgers-krijgen-recht-online-data-laten-verwijderen.html.

[82] European Commission 2012, p. 6-7. See also Recitals 53, 121 and 139.

[83] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, p. 46.

proposed Article 80, which intends to reconcile the fundamental rights of *data protection* and freedom of expression.[84]

> **Article 80 Processing of personal data and freedom of expression**
>
> 1. Member States shall provide for exemptions or derogations from the provisions […] in Chapter II, […] III, […] IV, [….] V, […] VI, […], VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.
>
> 2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 […].[85]

Thus Article 80 by itself will not be able to prevent a negative impact on freedom of expression of the possible strengthening of the right to have deleted in Article 17. It will depend on the exemptions and derogations implemented in the Member States. Generally, Article 80 gives rise to the following crucial questions that determine the extent to which data protection will negatively impact on freedom of expression.

(1) Who will be able to invoke the exemptions and derogations implemented at the level of the Member States and for which processing operations?

(2) And what exemptions and derogations can be expected at the level of the Member States, considering the text of the GDPR as well as the right to freedom of expression?

The first question involves interpreting who will be able to claim that certain "processing of personal data [is] carried out solely for journalistic purposes or the purpose of artistic or literary expression". The second question will depend on the Member States, as well as their margin of interpretation under the proposed rules as well as the right to freedom of expression. For the answer to both questions, some clarification can be found in the EC communications with the proposals as well as recital 121:

> (121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or

[84] Notably, this is different than balancing the right to privacy with freedom of expression, something which is prevalent in press, media, tort, and portrait law at the Member State level.
[85] GDPR.

> international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.[86]

As can be seen, the phrase 'journalistic purposes' has been retained in the proposed text of Article 80, which is somewhat surprising. The *Satamedia*-case, where the CJEU gave its interpretation of Article 9 of the current Directive, established that the media exception must be interpreted broadly. The exception does not only apply to media undertakings, but to "*every person*" engaged in journalistic activities. In addition, journalism should not be understood in the 'classic' sense: according to the Court, it is not the medium that is decisive, but the object of the publication, namely "disclosure to the public of information, opinions or ideas."[87]

The Explanatory Memorandum to the proposal indeed refers to *Satamedia* and Recital 121 above mentions the relevant considerations.[88] This raises the question why the text in Article 80 itself was not altered in a way that better reflects this broader interpretation to secure a more uniform and modernized interpretation of the scope of Article 80's instruction to the Member States in which contested notions such as 'journalism' do not play a decisive role. In view of the aim of the Commission to modernize the rules this is unfortunate. What about bloggers, discussion forums, online archives and information delivered through mobile apps? And are intermediaries like search engines and social media (and some of its users) eligible? And what is the position of new services that contribute to the public debate, such as DocumentCloud, which is based on open data journalism?[89] Recital 121 does contain the wording derived from the Satamedia ruling but also clarifies that Article 80 should in particular apply to news archives and press libraries, which again seems to target the more 'traditional' media.[90] In view of this, the EDPS may be right to suggest deletion of the wording 'solely for journalistic purposes' as it has no real value anymore as a consequence of the *Satamedia*-ruling.[91]

What is perhaps even more striking is that Article 80 does not in any way clarify what needs to happen at the level of the Member States. Article 80(1) does not state which exemptions or derogations there have to be made at the Member State level. It also does not prescribe which exceptions would be undesirable.[92] It only contains the instruction to the Member States to "provide

[86] GDPR.

[87] CJEU 16 December 2008, C-73/07 (*Satamedia*), par. 58-62.

[88] European Commission 2012, p. 15.

[89] See http://www.documentcloud.org/home, further discussed in section 4.2.5.

[90] See Recital 121.

[91] European Data Protection Supervisor 2012, par. 286.

[92] After listing all the possible chapters, recital 121 states that "[t]his should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation." Seemingly, Chapters IV (Controller and Processor) and VII (on co-

for exemptions or derogations". In the proposed Article 80, this has to happen with respect to *all* relevant Chapters of the Regulation, but which provisions and in what way they should not be applied or applied differently due to freedom of expression concerns is unclear.

This problematic amount of space for interpretation by the Member States will likely be the cause of much legal uncertainty for online services involving the public processing of personal data. The legal uncertainty will likely be the cause of chilling effects on online services that would like to invoke Article 80 but can only do so successfully in a number of countries. For example, whether Article 17 is applicable will then have to be assessed on a national, possibly case by case basis. In this sense, it is surprising that the European Data Protection Supervisor "fully supports the flexibility given to Member States under Article 80 to put in place exemptions or derogations from the provisions of the Regulation".[93] It is likely that this legal uncertainty will impact smaller online media and services more heavily, since dominant services can be expected to manage the legal risks better.[94]

This flexibility on such a crucial aspect of the regime is also very hard to reconcile with the fact that Article 80 is part of a Regulation (and not a Directive) and the overarching goal of harmonization more generally.[95] In principle, a Regulation does not need implementation in national law, but is directly applicable and "binding in its entirety".[96] Still, Article 80 explicitly requires legislative action regarding exceptions: member states "shall notify to the Commission those provisions of its law which it adopts". Apparently, member states have two years after the entry into force of the Regulation to put in place the appropriate legislation.[97]

In addition to Article 80, Article 83 contains an exception for 'Processing for historical purposes'. Similar the current Directive, 'historical purposes' are listed together with 'statistical' and 'scientific research' purposes. The exact scope and meaning of these purposes is however not defined in the Regulation. This may result in the same delineation problem as 'journalist' or 'journalistic'.[98] The question whether there is processing for historical purposes is of importance to determine whether the exception in the proposed Article 17(3)(c) is applicable.[99] Under that exception, data that normally should be erased, may be retained insofar as "necessary [...] for historical [...] purposes in accordance with Article 83".[100]

There is not much to be found in the legal literature about the scope and substance of the 'historical purposes exception' in the Directive, such as case-law on the interpretation under the General Directive. In view of this, the proposed Article 83(3) is important, which states that the Commission is

---

operation and consistency) were later added to the text of the final proposal of the EC and this sentence could have been deleted.

[93] European Data Protection Supervisor 2012, par. 283.

[94] Compare Joris van Hoboken, 'Search engine law and freedom of expression: a European perspective'. In K. Becker & F. Stalder (Eds.), Deep search: the politics of search beyond Google (85–97). Innsbruck: Studienverlag, 2009.

[95] See also Hins 2013, supra note 73.

[96] See http://europa.eu/legislation_summaries/institutional_affairs/decisionmaking_process/l14522_en.htm.

[97] See proposed Articles 80(2) and 91.

[98] See A.W. Hins, 'Wat is een journalist?', *Mediaforum* 2008-5, p. 189-190; T. Schiphof, 'De onduidelijke journalistieke exceptie in de Wet bescherming persoonsgegevens', *Mediaforum* 2008-5, p. 208-211.

[99] It should be noted that the same phrase of "historical, statistical or scientific research" is used in other proposed provisions as well; see Article 5(e) on 'Principles relating to personal data processing', Article 6(2) on 'Lawfulness of processing' and Article 9(2)(i) on 'Processing of special categories of personal data'.

[100] In the same sense: proposed Recital 53.

authorized to "adopt delegate acts [...] for the purpose of further specifying the criteria and requirements for the processing of personal data" for amongst others historical purposes. These delegate acts may also specify the "necessary limitations on the rights of information to and access by the data subject".

Hence, the precise interpretation of the historical purpose exception will emerge in practice. To get an idea of the discussions that are likely to take place it may be instructive to look at some of the responses in the earlier consultations. In this context, the National Archives of England stated that the right 'processing solely for historical research purposes' could be defined as "processing [that] consists solely of preservation of archives that are not yet available to members of the public for research".[101] The National Archives further distinguishes data processing that is used to make decisions relating to data subjects from this type of processing, which "can be of significant value for future historical research" and "it should continue to be possible for these personal data to be preserved as archives".[102]

But the changing practices of online archiving may lead to interpretation issues here as well.[103] The National Archives of England also points at a "new way of undertaking historical research", namely by remote access. In this form, researchers do not visit archives but access digitized copies from their home. Does this mean that online archives can invoke the historical purposes exception too? Although proposed Recital 121 explicitly mentions them – together with the audiovisual sector and press libraries - only in relation to 'journalistic purposes', they have a historical function as well, namely preserving historical records. Another organization, A&N Media, mentions records of "statements made by public figures, politicians, opinion formers" as examples; these records "must be able to be preserved with integrity".[104] This indicates the actual interrelationship between the exceptions in relation to Articles 80 and 83.

Can Article 80 in conjunction with Article 17(3) still be invoked if the purpose is not only journalistic but also historical? In addition to new archives, mention can be made of photographic libraries that "provide important historical records" and "function as vital resource of high-quality news content".[105] This consideration reflects the ECHR judgment in *Times v. U.K*, in which the ECtHR recognized the

> "substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research […]".[106]

This convergence between media and archives in the context of the Internet is striking and could be better recognized in the new data protection framework.

---

[101] The National Archives of England, response to Com(2010) 609 final, 12 January 2011 available at: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/natarchives_uk_en.pdf.

[102] The National Archives of England 2011.

[103] See also Section 2.

[104] A&N Media, response to Com(2010) 609 final, 13 January 2011, available at: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/a_and_n_media_en.pdf.

[105] European Publishers Council, response to Com(2010) 609 final , 15 January 2011. available at: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/epc_and_annex1_en.pdf.

[106] *Times v UK*, par. 45 (emphasis added).

6. Current Debates in the EP and the Council about the Right to be Forgotten

The GDPR is currently the subject of discussion in the European Parliament and the Council. The right to be forgotten and Article 17 is one of the most discussed elements of the proposals. In the European Parliament a very large amount of amendments has been tabled with respect to Article 17 and related recitals. To a lesser extent, this is also the case for Article 80. The Council has by May 2013 produced a seemingly complete overhaul of the right to be forgotten and the right to erasure. This makes it likely that any text that will finally be adopted with regard to specific rights to have personal data erased will be quite different from the original proposals by the European Commission.

Furthermore, and ultimately more important is that several of the basic principles and definitions in data protection are the subject of intense debate. For instance, a set of proposals has been tabled in the EP that would introduce what could be called 'data protection light' for so-called pseudonymous data, that would alleviate the requirements for invoking a legitimate interest as a basis for processing, or those for obtaining consent. These proposals, even more than the precise text of Article 17 could seriously affect the extent to which data subjects could be said to exercise control over their personal data or request their deletion, be it in closed databases or published online.

When looking at Article 80, the question is whether any further specifications of the scope and implications will be agreed upon. Its wording in the proposal may already reflect the reality that it is hard to come to agreement between the Member States of how to define processing operations that should be the subject of derogations or exceptions, as well as the cultural differences in the relative value attached to freedom of expression, data protection, privacy and human dignity. There are amendments that propose to delete the reference to journalistic purposes in return for more general references to freedom of expression, such as Amendment 324 on Article 80 from the Albrecht report.[107] There are also amendments that propose to give the EDPB a possibility to give guidance on which derogations and exceptions are necessary, which could be a good compromise to obtain some degree of harmonization.[108] Notably, there are also amendment to Article 80 that would make most of the Regulation inapplicable to processing for journalistic purposes.[109] Clearly, this solution would put even more weight on the determination of what can be considered processing for journalistic purposes. For many Member States, including Germany and the Netherlands,[110] this would lead to more far-reaching exemption of the media.[111]

When looking at Article 17, it becomes apparent that this Article has become one of the most discussed proposals in the Regulation. In the Albrecht report alone there are more than ten amendments dealing with Article 17 and related recitals and when looking at all the Amendments proposed, much more than hundred (of the total of around 4500) deal with Article 17 in some way.[112] As mentioned above, the Council seems to have developed a complete overhaul of Article 17 and the Council document lists a long list of reservations, questions and arguments against specific

[107] See Committee on Civil Liberties, Justice and Home Affairs, Jan Philipp Albrecht, Draft Report, 16 Januaruy 2013.

[108] See Amendment 879 in ITRE.

[109] See e.g. the Amendments proposed in LIBE by Voss, Kelly, Van der Camp et al. Interstingly, they also propose to delete the clarifications in recital 121, including the wording taken from the *Satamedia* ruling. In other words, the implications of the media exception are clarified but the scope is unclear.

[110] See Article 3 Dutch Data Protection Act (Wbp).

[111] See supra note 73 for a short discussion of the media exception currently in place in several Member States.

[112] See ParlTrack, Dossier 2012 0011 COD, http://parltrack.euwiki.org/dossier/2012/0011(COD)

elements of the original proposal.[113] In the European Parliament, there seems to be quite some support for the deletion of the right to be forgotten from the title of Article 17 and the deletion of Article 17(2). In other words, it is possible that the end result may not involve a 'right to be forgotten' in any form or add any new elements specifically related to 'public information'. This would bring the end-result closer in line with the current Directive.

For Article 17(2), it is unclear what will be the end-result. Amendments propose to delete or add specific elements in ways that sometimes lead to completely new provisions (i.e. the problem that ends up being solved becoming a completely different one) and are often incomprehensible to the author of this report. Some amendments propose to delete the criteria that data has to have been made public, thereby broadening the scope. Some propose to include processors and others turn the provision back into an obligation to get data removed instead of an obligation to inform.

The Council document from early May 2013 that was recently discussed publicly by civil society groups, such as Netzpolitik in Germany, contains an overhaul of the proposed right to be forgotten and erasure.[114] The Council has chosen to make Article 17(4) from the proposal about the restriction of processing of personal data into a separate Article 17a. Notably, the new Article 17a does not (yet) entail a specific freedom of expression exception such as Article 17(3) of the EC proposal, even though it could lead to obligations to block access to content online. The Council's current wording for Article 17 contains the main elements discussed in this report, relating to Article 17(1) and 17(2) from the proposal. In addition, Article 17b contains a notification obligation for controllers to third parties when data have been erased or rectified. Interestingly, the Council document contains ample reference to the possible negative impact of Article 17 on the right to freedom of expression in the comments by the Member States.

7. The Right to be Forgotten and Other Laws related to Online Publishing

What is often overseen in the discussions about the right to be forgotten that are currently ongoing, is that there is already another set of laws in place that regulate the legality of making information about others public. Tort, press, and portrait law in the Member States, for instance, entail intricate doctrines to balance the interests in society in the publicity of and about others and the interests of privacy and dignity of natural persons.[115] At a fundamental level these doctrines need to strike a balance between the fundamental rights at stake: the right to privacy and the right to freedom of expression. There is quite some divergence in the way this balance is struck in different parts of Europe, a divergence that reflects difference in attitudes as regards privacy, reputation, dignity and the value and meaning of freedom of expression.

The convergence in the use of the Web and specific online platforms for serious public debate, semi-private socialization and various forms of commerce as a result of the digital transition raises the question about the proper scope of application of these doctrines that were traditionally reserved for

[113] Council Presidency, 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) - Revised version of Chapters I-IV, 6 May 2013, available at https://netzpolitik.org/wp-upload/2013_05_06council_comix_et_al-8004-13-2.pdf.

[114] See https://netzpolitik.org/2013/exklusiv-wir-veroffentlichen-verhandlungsstand-der-datenschutzreform-im-ministerrat-minister-schutzen-markt-aber-keine-daten/

[115] It goes beyond the scope of this research to discuss these laws in detail.

the institutionalized press. It also raises the question where these doctrines should start and where data protection should end, and to what extent overlap of rules should be possible and accepted. There have been quite some cases already in which judges had to resolve the concurrence of these specific laws relating to publicity and general data protection.[116]

The root cause of this legal concurrence is the omnibus character of EU data protection rules and the wide scope of its principal definitions. The definition of processing includes publication and any processing activity involved in the further circulation. The definition of personal data includes all information relating to or about natural people as long as they directly or indirectly identify the data subject.[117] As soon as one starts writing about someone using a name, or the posting of pictures, there is processing of personal data. The real reason for the concurrence, however, is that all processing of personal data is covered "if it is automated", or in other words "wholly or partly by automatic means" as is stipulated in Article 3(1) of the current Directive. In the context of old analogue media, the personal data contained in publications was typically not covered, but on the Web, every operation with regard to data *is taking place with automated means*, implying that all processing of personal data, regardless of the quantity is basically covered in a new electronic media context.[118] This has made the application and scoping of the media exception in the Member Stares of course a more important question since there are much more processing operations for which online media would need to be able to invoke it to avoid full application of data protection rules.[119]

To illustrate the fundamental differences in approach between data protection law and the law related to the legality of publishing about others, it is instructive to look at a case involving the so-called 'Internet publication rule'. This is the case of *Times v. UK* at the ECtHR decided in 2008.[120] In this case about the protection of media against defamation lawsuits after a considerable lapse of time, the ECtHR for the first time qualified the importance of the Internet for the promotion of the values protected by Article 10 ECHR.

> "In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10."[121]

What is so interesting about this case is the fact that it resolves around protecting the media *against* claims with regard to old publications. The idea behind the 'publication rule' is that after some time media should not have to fear for litigation with respect to the legality of their publications. Even though the ECtHR does not set a strict limitation period for pursuing legal action against a publication, it does stipulate the need for some limitation in this regard at the level of the Member States.

---

[116] In the Netherlands, see e.g. Hof Den Bosch (*kleintje muurkrant*). See also supra note 73.

[117] See Article 29 Working Party, Opinion on the Concept of Personal Data, 2007.

[118] This result became apparent after Lindqvist, CJEU 6 November 2003, C-101/01 (*Lindqvist*).

[119] See CJEU 6 November 2003, C-101/01 (*Lindqvist*).

[120] See ECtHR 10 March 2009, *Times v. United Kingdom.*

[121] ECtHR 10 March 2009, *Times v. United Kingdom*, § 27 (adding that ''[t]he maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10'').

> "[The Court] observes that the introduction of limitation periods for libel actions is intended to ensure that those who are defamed move quickly to protect their reputations in order that newspapers sued for libel are able to defend claims unhindered by the passage of time and the loss of notes and fading of memories that such passage of time inevitably entails. In determining the length of any limitation period, the protection of the right to freedom of expression enjoyed by the press should be balanced against the rights of individuals to protect their reputations and, where necessary, to have access to a court in order to do so. It is, in principle, for contracting States, in the exercise of their margin of appreciation, to set a limitation period which is appropriate and to provide for any cases in which an exception to the prescribed limitation period may be permitted […]."[122]

In other words, from Article 10 ECHR it arguably follows that those responsible for making information public online should at some point no longer be haunted by the prospect of legal action against the publications legality. Clearly, this is precisely the opposite logic as underlying the right to be forgotten in data protection, as applied to online publications. In the latter case, the 'older' the publication becomes the less reason there is for it to stay online, at some point giving rise to the possibility exercise the right to be forgotten.

There are many more contrasts to be found when comparing the data protection approach to online publications and the approach that follows from media and tort law principles as developed with respect to paper-based media. Many of these contrasts relate to the different dynamics between paper-based and electronic Web-based media. In a paper-based media world, publications would quite quickly go out of circulation and become de facto hidden from societal view. They would of course remain accessible in certain newspaper (or personal) archives and libraries, but they would obtain a practical obscurity that alleviated the concerns now present with relation to historic publications online.

But where do an online medium's publications become historic publications that are part of its Internet archive? It is worth considering that in the context of online media, every publication is in some sense historical and online media are inherently archival in nature. Acrhiving, understood as the keeping available of publications for an online audience, seems to be the standard practice, taking place with the use of the same architecture as the one used for new ones. Is a new publication that is still online after 1 month part of the archive? And after 2 weeks, 34 hours or 15 minutes? In other words, the online information offering by definition consists of the historic record of publications that is kept available for online consumption, often categorized in dossiers related to certain specific topics and themes of interest and together with internal and external search functionalities.

From the perspective of freedom of expression and the effective exercise of the right to be informed, a clear added value of the electronic environment is precisely that the information offering of media is steadily growing as time passes. The whole of historic and current publications about a specific topic (possibly involving personal data) gives users the ability to put current and historic affairs and public figures into context. The use of hyperlinks and permalinks makes it possible to facilitate access to historic publications in new ones and to integrate new publications into the existing structured

[122] ECtHR March 10, 2009, *Times v. United Kingdom*, § 46.

network of online information.[123] This makes the distinction between online media and their archives difficult to make.

Another contrast between media law and the right to be forgotten in data protection exists with respect to the crudeness of the measure to deal with the potential harm of historic 'publications'.[124] The primary way of dealing with information under Article 17 GDPR, is to delete it or make it inaccessible.[125] In the context of online media, the press and press archives, more granular methods have been developed, such as the right to rectification, the annotation and placement of messages and the right of reply. The fact that more granular and proportional measures for dealing with the anxieties and harm that people invoking the right to be forgotten may experience are absent in Article 17 GDPR, could be proof that it deserves much more scrutiny before being adopted for public information on the Internet. In fact, this could be taken as an argument against the use of the current data protection framework to address issues with respect to publicity, which other legal doctrines may be better equipped to tackle.

If anything, the issues with the accessibility of online 'archives' (and the personal data therein) seem to arise due to the effectiveness of search media in crawling, indexing and ranking the information offering available online. Ironically, it may be the effectiveness of search giving access to historic publications which increases the pressure on information providers to remove controversial/contested historic publications, thereby impacting on the integrity of their collections. From the perspective of freedom of expression and the interests in keeping valuable truthful but controversial information online, this is something to worry about.[126]

8. The Right to be Forgotten and Intermediary Liability Regulation

As mentioned above a number of times, the right to be forgotten could be seen as a reaction to new forms of publicity facilitated by the online environment. More specifically, the right to be forgotten seems to be constructed in relation to two types of intermediaries, namely search engines as well as social media. Social media give permanence to utterances, conversations and personal stories, in a way that make them often retraceable to large or even unrestricted groups of users. Search engines greatly diminish the practical obscurity of information online and can facilitate the accessibility of information and ideas of questionable quality. Information that is traditionally made public mandatorily, such as public records containing personal information, is now more easily accessible. Information which was not traditionally published at all, such as conversations and debate between readers in reaction to news and current affairs, has found permanence on blogs, message boards and comment sections.

How has the law generally dealt with the harm intermediaries may cause in facilitating access to unlawfully published personal data and other harmful publications? For search engines, looking at the case law in the Member States and at the EU level, the general rule is that they are not to be held liable for linking to unlawful information online as long as they have no specific knowledge of the

[123] See also Joris van Hoboken, annotation to ECtHR March 10, 2009, *Times v. United Kingdom*, Mediaforum 2009.

[124] Meaning information that is publicly accessible online (not necessarily published by 'the media').

[125] See Section 3, 4 and 6.

[126] See Van Hoboken 2012.

unlawful nature of the information concerned.[127] This is the so-called safe harbor regulation from the Ecommerce Directive, which applies to intermediaries such as internet broadband (mere conduit) and hosting providers. Generally, social media can also invoke the hosting safe harbor in Article 14 of the ECD for the data posted by their users.[128] The precise status of search engines under this regulation is still hotly debated in Europe, but in the context of the discussions about the scope of the safe harbors there is general agreement that search engines cannot be asked to take pro-active responsibility for the legality of the information in their index or search results. This rule applies to copyright or trademark infringements and to substantive restrictions relating to privacy and reputation protection. In principle, the rule should also apply in relation to EU data protection rules applied to online publications of personal data. In other words, even if a publication of personal data would be unlawful, a search engine would only have to remove it after being notified and able to establish that the information is actually unlawful.[129]

The current Directive does not contain provisions relating to online intermediaries. This does result in a rather unclear situation regarding the obligations of intermediaries such as search engines with respect to personal data in their ordered indexes. In the absence of a clear rule, the Article 29 Working Party concluded on the basis of proportionality that search engines should in general not be considered the primary controllers of the personal data in their index. At the same time, certain national DPAs, the AEPD in particular, have since long held that search engines are to be considered controllers of the personal data in their index.

In the GDPR, Article 2(3) provides that "this Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive." However, this does not really answer the question whether search media could still be considered controllers of the personal data in their index and thereby responsible for complying with data protection rules with respect of such data. For instance, the safe harbors in Directive 2000/31/EC still leave room for injunctions and administrative orders.

The classification of search engines as controllers of personal data would have a number of consequences. First, Article 17(1) could become directly applicable to search engines, depending of course on the question of how Article 80 would have been implemented in the particular Member State. In other words, search engines would become directly responsible for the content of certain search results containing personal data, while normally search media would only fall under secondary, contributory liability regimes. Second, it would make it possible in theory that injunctions are imposed on search engines to remove personal data from the index, even though the publication of the personal data at the source would have to be considered legal.

What is missing in the current 95/46 Directive is a provision such as Article 5(1) in the Information Society Directive, which provides for a mandatory exception to transient copies (e.g. made by intermediaries) and a clarification of how to establish who should be considered the controller in the

[127] For a detailed discussion of search media from the perspective of intermediary liability, see idem.

[128] See recently CJEU 16 February 2012, C-360-10 (*SABAM v. Netlog*).

[129] In practice, such rules may cause chilling effects since a search engine may want to play safe and remove every piece of information of which it is notified. This is a long standing concern in the context of intermediary liability standards. See e.g. Chilling Effects, www.chillingeffects.org.

context of online intermediary activities.[130] But the problem is that the current data protection framework doesn't perform well with respect to the reputational and privacy issues facilitated by online intermediaries. When looking at online services such as social media and search engines, the data protection regime's basic principles still function relatively well with respect to the regulation of the relationship between the services and their users. The Article 29 Working Party managed to develop a relatively clear interpretation of the data protection norms as applied to the collection and use of *user data* in this context. The real problems emerge with respect to the mediation of public and semi-public information flows facilitated by these services and the corresponding relation of these services (and their users) to third party data subjects under data protection law.[131]

In other words, a first step in coming to a clarification of the responsibilities under data protection law of services that have an intermediary character could be to make a distinction between the processing of personal data in the relation between users and the service (user data) and the processing of data on or through the service (content data). As mentioned, the first type of relation seems more suitable to be structured through the application of data protection rules and principles. Hence the first step would at least separate the hard issues relating to content data from the relatively easier ones.

A second step would be to determine the extent to which the service provider would have to be considered a controller. As regards the second type of data, it is likely that users and third parties can be considered co-controllers in one way or another, raising the question about the scope of the household exception.[132] Completely passive intermediaries should normally not have to be considered a controller at all. For instance, a mere hosting provider does not know whether its customers have personal data stored on its services. Currently, there are situations in which the hosting provider would become a co-controller, for instance when it would decide to delete a database with personal data from its servers in response to a takedown request. This could be solved by stipulating that such merely facilitative processing should not lead to controller status.

A problem that has to be acknowledged in this regard, and which could make some form of data protection a potentially valuable framework for intermediaries also, is that intermediaries are less and less passive with regard to the personal data that are processed. This is the issue of value-added operations by intermediaries on the personal data in their platforms. An example would be the datamining of pictures by a foto-sharing service like Instagram for the purposes of better understanding the network of friends the user is part of. And another example would be the growing sophistication of person-search engines that are not at all agnostic of the type and categories of the data they find online or obtain in contractual relations with third parties. More fundamentally, the ambient technologies that are developed in view of interaction with humans may more and more be programmed to be aware of the presence of humans.

The Article 29 Working Party touches upon the issue in the context of search engines also.

---

[130] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22/06/2001, p. 10-19.

[131] See Helberger & Van Hoboken, supra note 10.

[132] See e.g. supra note 31.

> "Thus search engine providers may perform value-added operations linked to characteristics or types of personal data on the information they process. In such cases the search engine provider is fully responsible under data protection laws for the resulting content related to the processing of personal data. The same responsibility applies to a search engine that sells advertisement triggered by personal data – such as the name of a person."[133]

A third step would be to determine the extent to which the service providers could invoke the media exception pursuant to Article 80 with respect to the processing of content data. Currently, Article 80 seems to have been written with publishers in mind. But how to deal with the intermediaries that help these publishers find a way to an audience, like search engines? In the end, these are the services that establish our digital horizon. Would it not make sense to provide space for intermediaries to invoke the same exception for the processing of personal (content) data on their platforms? If an information provider like an online newspaper can invoke freedom of expression safeguards for the processing of personal data in its articles, it surely makes sense to give intermediaries a similar derivative defense. And how to deal with the platforms that provide users a space to communicate with very small to very large audiences? For better and for worse, the effective exercise of freedom of expression of everyday citizens, politicians, activists, journalists and artists has become dependent on the operations of these platforms and their willingness to harbor conversations about matters of private and public importance. The convergence of these different conversations (that do contain personal data of all sorts) in one networked environment should not mean that the rule set developed for one of them is applied to the other without carefully taking into account the negative consequences this could have for freedom of expression.

9. Conclusion

The right to be forgotten has stirred up the debate about the new data protection rules at the EU level considerably. And the right as a concept has a rich legal history already. In this report, the actual proposals of the right to be forgotten have been discussed in detail, looking at the potential impact of this right to have information deleted on freedom of expression. On the basis of the analysis it must be concluded that currently, the right to be forgotten does not add much in comparison to the current framework. The new elements with respect to public information in Article 17(2) are likely to be inconsequential for data protection practice. The real impact on the possibility of data subjects to exercise some control over 'their' personal data will likely stem from the implementation of the basic principles and definitions in the new GDPR.

The impact of the right to be forgotten on freedom of expression will – if the proposals are adopted without major change – depend on implementation of Article 80. This provision which is meant to safeguard freedom of expression, but its lack of clarity about the scope and substance of exceptions and derogations to be made in view of freedom of expression raises very serious questions. In a time in which online media are ever more automated and converged with non-traditional information society services, this is a real concern. Divergence at the national level will cause legal uncertainty that is bad for the internal market and can lead to chilling effects on freedom of expression. It is important that Article 80 will do justice to the current state of electronic media, archives and practices and this is not something that can be left completely to the Member States.

[133] See supra note 52.

It must be stressed that data protection is not the only way to address the issues of online publicity. Even if data protection rules would not apply, most issues with respect to the harm people may experience as a result of online publicity could be addressed through the application of tort laws, media laws and press laws. These laws have different approached to striking a balance than the data protection framework, which could be more sensitive to freedom of expression concerns due to a long history of legal development and case law. The same can be said about the doctrine of intermediary liability. The right to be forgotten in data protection law has a clear relation with search engines, but proposals that make search media responsible for the personal data they process are hard to align with the principles underlying intermediary safe harbors. The data protection regime does not contain an intermediary responsibility exception itself and neither is it clear to what extent intermediaries will be able to invoke the media exception. Generally, it must be concluded that the interface between intermediary liability, data protection and freedom of expression needs very careful scrutiny, since the processing of personal data by intermediaries in ever more intelligent ways, both impact the informational autonomy as well as informational privacy of internet users.

European Commission
EUR 26410 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember

Author: Joris V.J van Hoboken

2013 – 30 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-35010-8

doi: 10.2788/51998

Abstract

This report puts the EC proposal for a right to be forgotten in context and discusses it from the perspective of freedom of expression. As will become apparent, the right to be forgotten as proposed in data protection law is a concept that relates closely to the regulation of privacy harms caused by new forms of publicity online, most notably search engine and social media publicity. These new forms of publicity are the subject of daily news reports about the privacy impact of the Internet and related services Even though scientific literature shows that the Web is extremely volatile, that valuable information constantly disappears and that the structural preservation of historic publications online is a very hard problem, the perception that the Web never forgets seems to remain prevalent.

Acting on concerns over online publicity, over the last decade, Data Protection Authorities (in France, Spain and Italy in particular) have laid the foundation for the establishment of strengthening the control of people over the public data that is processed about them online through a so-called 'right to be forgotten'. The European Commission, after consulting on the topic, has made the name and (some parts of) this right into a central element of its proposal for a General Data Protection Regulation. Considering the fact that these proposals relate to new forms of publicity online, a fundamental question is whether freedom of expression is sufficiently taken into account. Much of the public debate in the general media that has taken place over the last two years about the right to be forgotten touches on this important question, that will be addressed in this report through a discussion of the proposed Article 17 and 80 and related legal doctrines. The EC proposals are discussed in detail, taking into account recent developments in the European Parliament and the Council.

The EU data protection framework seems to have become the most important legal framework for addressing privacy concerns relating to online media. This report also addresses the fundamental question to what extent this is a good development. It does so by first looking at the interface of data protection as applied to online publications of personal data and the laws at the national level relating to the lawfulness of publishing about natural persons. Second, and finally, this report looks at extremely (and ever more) complex interface of data protection with intermediary liability regulation at the EU level (limited safe harbors) and the Member States (secondary liability). Data protection law currently lacks the tools for setting the boundaries for intermediary and the current proposals do not effectively address this issue either. This raises the question of how this interface could be better established, which will be addressed in the final part of this report.

Section 2 will discuss the backgrounds of the right to be forgotten. Section 3 discusses the already existing principle and the implied right of erasure under the current Data Protection Directive. After that, the EC proposal for a right to be forgotten in Article 17 of the Regulation will be addressed (Section 4), the way data protection deals with freedom of expression concerns in Article 80 and recital 121 (Section 5) as well as some of the proposals to amend Article 17 and 80 by the European Parliament and the Council (Section 6). Section 7 discusses the interface of data protection with privacy tort law and media law and Section 8 discusses the interface with intermediary liability regulation. Section 9 concludes.

LB-NA-26410-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.