The European Approach to Privacy

van Hoboken, J.

DOI
10.2139/ssrn.2418636
Publication date
2014
Document Version
Submitted manuscript
Published in
2014 TPRC Conference (archive)

The European Approach to Privacy

Joris van Hoboken[1]

DRAFT

ABSTRACT: This paper critically assesses the character of European (Union's) privacy law and policy in the field of online media and electronic communications. Contrary to current understanding, this field of law is more fragmented and ill-developed than is often assumed, in particular by those discussing privacy law and policy in an international and transatlantic context. In fact, some of the most challenging regulatory issues in the field of online media and electronic communications still lack a well-developed common European approach and remain the subject of regulation at the level of the different member states of the European Union. Drawing on historic insights, the paper shows how EU policy making in the field of privacy and data protection is and remains strongly influenced by the EU institutional setting. In particular, the paper shows that the specific substantive outcome of European privacy law and policy is strongly influenced by and can only be understood properly through the lens of the ongoing project of European integration more generally.

The paper will develop its main thesis by focusing on three important and current privacy issues and their treatment by EU lawmakers and the EU legal system. These are: (I.) the question of retention of communications meta-data (e.g. traffic and location data) in the field of electronic communications; (II.) the legal framework for liability of search engines for privacy and reputational harms in the online environment, including a 'right to be forgotten', and (III.) the question of the security of and the potential lawful access by foreign governments to data in the cloud. After discussing these substantive privacy policy issues and the legal frameworks that have developed (and are developing) to address them at the EU level, the paper will analyze these frameworks in view of the apparent interplay of the substance of privacy law and policy at the EU level on the one hand and the broader constitutional and institutional dynamics related to EU competency and integration.

The paper starts with a discussion of the basic underlying motivations, rationales and competences for addressing privacy issues at the European level, which until recently were predominantly economic in nature. The implication of this is that some of the most pressing data privacy issues which are primarily non-economic in character, have been addressed at the fringes of what could be called the European approach to data privacy, in which the establishment of a functioning European internal market and the free flow of personal data under sufficient safeguards relating to data privacy are the dominant concerns. More recently,

[1] Dr. Joris V.J. van Hoboken, Microsoft Postdoctoral Research Fellow, Information law Institute, School of Law, New York University. All comments welcome and can be sent to jvh3@nyu.edu. The author would like to thank PLSC 2014 and those present at the presentation of this paper for their valuable comments and feedback to an earlier draft of this paper.

the adoption of the Lisbon treaty, the establishment of a binding right to data protection and privacy in the EU Charter and a new legal basis for the establishment of data protection rules at the EU level, EU privacy law and policy has become increasingly connected to the furtherance of the protection of privacy and data protection as fundamental rights more generally. Through the case studies in the paper, this dynamic of how policy rationales end up playing out at the EU level and inform the substance of privacy policies adopted, is illustrated in detail. In particular, the analysis shows how EU policy making tends to strive towards a common and comprehensive European approach, but typically fails to take account of some of the leading concerns, and is often simply not equipped or even allowed to include them in the process. For instance, there is significant disagreement about the weight that should be attributed to freedom of expression concerns in the online environment and the role of the EU with respect to media and the proper balancing of freedom and privacy in the media remains limited. With respect to national security concerns there are no European harmonization of national approaches at all.

The result is that important policy concerns from the perspective of privacy in electronic communications end up being addressed indirectly, inefficiently and incompletely, through the European data privacy frameworks that may aspire to be comprehensive but would need significant reforms to achieve this aim. The article will discuss possible reforms but will warn against aspirations of further harmonization and unification of European Privacy Law. In the absence of fundamental institutional reform of the EU, further harmonization could end up being detrimental to other important policy goals currently addressed largely outside of the EU legal framework, including the issues of media freedom, criminal procedural justice and the protection of privacy and information security in relation to foreign intelligence agencies specifically discussed in this paper.

Table of Contents

1. Introduction

1.1. General introduction

European privacy law has received significant attention from outside of Europe, has had significant influence on the adoption of privacy laws around the world and features widely in the debate about privacy, both positively and negatively, as an important model for regulating privacy issues.[2] The recently concluded Big Data Report of the White House summarizes the European Approach as follows:

> "The European approach, which is based on the view that privacy is a fundamental right, generally involves top-down regulation and the imposition of across the board rules restricting the use of data or requiring explicit consent for that use."[3]

From a U.S. perspective, the European approach to privacy leads to continuing tensions and necessitates renegotiations of the frameworks with respect to emerging privacy issues, both in the public and the private sector.[4] The EU's adequacy requirements in the Data Protection Directive (DPD),[5] the Safe Harbor framework negotiated in the end of the 1990s, and the more strict approach to industry regulation of personal data use are primary drivers for continuous transatlantic debate and lobbying on these issues on the European side. On the other side

[2] See generally, Colin Bennett and Charles Raab, The Governance of Privacy, Policy Instruments in Global Perspective, Cambridge, MA: The MIT Press, 2006; Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press, 1995, at 195; Helen Nissenbaum, Privacy in Context, Technology, Policy and the Integrity of Social Life, Stanford: Stanford University Press, at 4; Joel Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 Iowa Law Rev. 497, 1995, at 500; Daniel Solove and Paul Schwartz, Information Privacy Law, Aspen, 4th Edition, 2011, at 1061 and further.

[3] White House Big Data Report, at 17.

[4] For a detailed discussion, see Paul Schwarz, The EU-U.S. Privacy Collision, Harvard Law Review, 2013. See also Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, Stanford law Review, 2000. For an early analysis, predating the DPD, see Joel Reidenberg, *The Privacy Obstacle Course: Hurding Barriers to Transnational Financial Services*, Fordham Law Review, 1991.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995, p. 31-50.

feature the interests of U.S. industry and government to establish favorable conditions for commercial data processing of European customers and governmental access to data respectively.

The continuous transatlantic debate and renegotiation between regulatory privacy models may sometimes obscure or give little attention to the actual diversity of approaches to privacy issues in the European context. In particular, data protection as a legal framework consisting of mandatory legal rules, and the codification of data protection and privacy as fundamental rights in the EU Charter has influenced the understanding of the European approach to privacy. What has less informed it, is the extent to which it is the product of a continuous and complicated negotiation of different approaches to privacy existing in the national legal traditions. More specifically, what seems underemphasized is that there is only partial harmonization through internal market harmonization and (data privacy) constitutionalization at the EU level. In many respects there is (still) no European approach to privacy and the European approach to the issues discussed in this Article clearly reflects that. In addition, the results at the EU level, i.e. the resulting course of Europe with respect to privacy, may often be the outcome of a process that has much less to do with the substantive regulation of privacy issues than with the European institutional and constitutional dynamics and general attitudes towards the European project of integration. This can be illustrated most sharply by looking at the different roles and attitudes of the dominant players at the EU level: the Member States, the European Commission, the Parliament and the Court of Justice of the EU.

1.2. Research Question and Methodology

This Article aims to contribute to the general question of what is the European approach to privacy really is. More in particular, it aims to contribute to the question of how the data protection framework and the fundamental right character of data protection in the EU Charter have become dominant in our understanding of European privacy and increasingly influential in the actual approach with respect to privacy at the EU level. Over the years, the European approach to privacy has been primarily shaped by the project of European internal market integration through harmonization. More recently, it has become characterized by the establishment, interpretation and enforcement of data protection as a fundamental right in the EU Charter, which allow for a potentially much broader scope of privacy law and policy making at the EU level.

To explore these issues and the answers to the questions above, the Article proceeds by analyzing three pressing privacy issues of in the field of electronic communications. These are: the question of retention of communications meta-data (e.g. traffic and location data) in the field of electronic communications (Section 3), the legal framework for dealing with privacy and reputational harms in search engines, including a 'right to be forgotten' (Section 4), and the question of the security of and the potential lawful access by foreign governments to data in the cloud (Section 5). These issues are selected on the basis of three criteria. First, they are complex and key privacy issues of our time that warrant significant debate and attention in

legal scholarship. Second, they are issues that have resulted in significant dynamics at the EU level over the last years as well as significant interaction with the legal approaches in other jurisdictions, most specifically the United States. And third, they are issues that lay on the boundaries of EU competency, thereby resulting in the dynamics the Article aims to explore: namely the dynamics relating to the interaction of European integration with substantive policy outcomes in the field of privacy law.

For each of these three issues, the Article first clarifies the privacy issue in substantive terms. Subsequently, it analyses the way these issues have been addressed at the EU level, with a particular focus on the interplay between the primary constituents in the EU law and policy making process, i.e. the European Commission (EC), the Member States, the European Parliament (EP) and the Court of Justice of the EU (CJEU). After having arrived at an understanding of the present outcome of the European process, the 'European approach' to these issues, this outcome is analyzed in view of the aim to understand the dynamics and policy rationales leading to this outcome.

Section 2 of the Article will provide some relevant background with respect to European privacy laws and starts with a discussion of the underlying motivation, rationale and competence for data privacy regulation at the European level. Initially, this has predominantly been an economic one, informing the establishment of the DPD in view of the functioning of the internal market. At the same time, in line with the understanding of data protection as related and connected to the right to private life, this framework purports to protect the fundamental rights of EU citizens. It will be briefly outlined that while the former rationale for EU policy dynamics is more definitely at the roots of the European Union project, there is reason to be skeptical about the extent to which fundamental rights are at the core of it, or are a necessary projection on and a defense of the European project.[6]

2. Backgrounds on the protection of Privacy and Data Protection in Europe

2.1. Data privacy rules at EU level

2.2. Privacy as a Fundamental Right

3. Data Retention

Data retention, i.e. the mandatory retention of data relating to electronic communications use in view of the availability for government agencies, has been one of the most hotly debated privacy issue at the European level for more than a decade.[7] The path of data retention is long

[6] On the relation of the EU to fundamental rights, see Alston and Weiler, An Ever Closer Union in Need of a Human Rights Policy: The European Union and Human rights, in; The EU and Human Rights (Alston, ed.), 1999; Charles Leben, Is there a European Approach to Human Rights, in; The EU and Human Rights (Alston, ed.), 1999, Williams, EU Human Rights Policies, A Study in Irony, 2004; Coppell and O'Neill, The European Court of Justice: taking Rights Seriously, Legal Studies, 1992.

[7] For a recent comparative overview of data retention obligations in the U.S. and in Europe, see Joel Reidenberg, The Data Surveillance State in the United States and Europe, Wake Forest Law Rev., Forthcoming.

and complex.[8] Starting in the 1990s, data retention was discussed in transatlantic working groups discussing law enforcement concerns with respect to new developments in electronic communications architectures. It became the subject of debate at the EU level in the early 2000s about an updated regulatory electronic communications framework that could have restricted the ability of Member States to adopt data retention laws nationally. Subsequently, a number of Member States started pushing for a so-called third pillar (Justice and Home Affairs) instrument in 2002.[9] In 2005, the policy process shifted to the first pillar (internal market harmonization) which led to the successful and record-speed adoption of a Data Retention Directive (DRD).[10] The DRD has been critically received in the legal orders of the EU Member States and by constitutional courts across Europe. As the EDPS has stated: "The [DRD] is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects."[11] While the CJEU in 2009 first upheld a challenge on grounds of EU competency, it recently invalidated it on fundamental rights grounds.[12]

3.1. The Privacy Problem

How to characterize mandatory data retention as a substantive policy issue? Shortly, the question is whether the possibility that electronic communications meta-data could be useful for government agencies should lead to the default storage of these data to ensure their availability for the government. Thus, data retention relates to the protection of privacy and communications freedom in view of government demands for the effective availability of data relating to the electronic communications of the people, including location data generated by mobile telephony use (meta-data). More specifically, data retention brings fourth the question of whether regulation should *ensure* that such meta-data should remain available for a certain period of time, in view of value of such data for the effective operation of government agencies on the one hand, and in view of the privacy and communications freedom on the other hand.

Thus, the following two questions are at the heart of a debate about the adoption of data retention laws. What is the actual value of meta-data for the relevant government agencies? What can be said about the proportionality of the interference of mandatory data retention with the rights to privacy, data protection and communications freedom? And more specifically,

---

[8] See e.g. Chris Jones & Ben Hayes (Statewatch), The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, SECILE Project, 2013, http://www.statewatch.org/news/2013/nov/Data-Retention-Directive-in-Europe-A-Case-Study.pdf.

[9] The European Union, established by the Maastricht Treaty in the early 90s provided for three EU pillars, the most important of which was the first one (the former European Community). The third pillar of the European Union provided for European law and policy making in the fields of law enforcement and judicial cooperation, a an area in which European integration was relatively minimal and the Member States retained most of their sovereignty.

[10] Data Retention Directive 2006/24/EC.

[11] See Peter Hunstinx, European Data Protection Supervisor (EDPS), "The moment of truth for the Data Retention Directive",Brussels, Dec. 3rd, 2010, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf

[12] CJEU 8 April 2014, Joined Cases C-293/12 and 594/12 (*Digital Rights Ireland*).

is it acceptable to mandate the blanket retention of all electronic communications meta-data, just because some of these data could end up having value in the future for government agencies?[13]

Fundamentally, the debate about data retention is also a debate about the proper government response to new technological developments that could impact the operations of government agencies, law enforcement and intelligence agencies in particular. To what extent can (certain parts of) government legitimately steer the design and adoption of technologies in society in the direction that it finds most favorable, while when left alone, the new technologies could positively impact the enjoyment of freedom and in society?[14] The Snowden revelations has shed new light on this question and the systematic efforts of intelligence agencies to increase their control over and investigative capabilities with respect to and on the basis of new communication technologies. With respect to the value of communications meta-data, recent reports have illustrated a wide variety of programs in which these data are the crucial target and subsequent intelligence resource.[15] Other documents show efforts with respect to new research and technology are aimed at "provid[ing] advanced knowledge of technology trends and opportunities to steer IT products and standards in a SIGINT-friendly direction".[16]

3.2. Towards European-wide data retention

How and why did data retention end up being addressed at the European level? As outlined above, the answer to this is a long and complex one. In the 1990s, initial discussions took place at the international and the European level about the lawful interception of telecommunications in view of the switch from traditional telecommunications to internet-based electronic communication systems. In these discussions U.S. authorities (the FBI in particular) played a central role in the formulation of substantive standards for telecommunications interception, standards that found their way into a European Council Resolution, silently adopted in 1995.[17] Public debate about the proposed requirements was absent; the EU constitutional structure put in place in 1992 did now allow for any meaningful

---

[13] Notably, this phrasing of the issue assumes that no bulk government access to all the data takes place under the relevant lawful access regimes. The Snowden revelations give some reason to believe that bulk access does take place. This makes prolonged retention in the private sector both less valuable and somewhat dubious.

[14] Compare Orin Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 2011. On the relation between technology, law and the enjoyment of freedom, see also Yochai Benkler 'Siren Songs and Amish Children: Autonomy, Information, and Law', 76 New York University Law Review 23, 2001.

[15] See e.g. the NSA's controversial meta-data program. For a discussion, see Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, January 23rd, 2014.

[16] The Washington Post, A description of the Penetrating Hard Targets project, last seen May 20th, 2014, http://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/#document/p2/a138768.

[17] Chris Jones & Ben Hayes (Statewatch), The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, SECILE Project, 2013, http://www.statewatch.org/news/2013/nov/Data-Retention-Directive-in-Europe-A-Case-Study.pdf. See also, EU Council, Draft Council Resolution on The Interception of Telecommunications, Brussels, Nov. 16, 1993, available at http://database.statewatch.org/e-library/1994-jha-k4-03-06.pdf.

scrutiny by the European Parliament. This changed in 2000, when the European Parliament was addressing the proposals for a new e-Privacy Directive, an internal market directive building on the data privacy regime established by the Data Protection Directive adopted in 1995 and replacing the e-Privacy Directive from 1997.

Data retention entered the debate about these directives concerning (data) privacy in the (liberalized) electronic communications sector in two ways. The existing 1997 Directive contained a provision obligating service providers to delete meta-data when they no longer served a regulated business purpose, i.e. service provision or marketing. The new proposal by the European Commission deleted this strict purpose limitation rules for meta-data, abolishing the regime that was typically characterized as 'data destruction' in the United States and was strongly opposed by the U.S. diplomatic representation in Europe.[18] In other words, the strict privacy rules for the private sector were opposed due to their impact on the availability of data for government agencies, while the direct regulation of such availability and the standards under which private sector data would be available to relevant government agencies at the national level were beyond the scope of the proposals.

The new e-Privacy Directive was also to contain an exception in view of law enforcement and national security, similar as the directive it replaced. The debate about the proper scope and language of this exception allowed the European Parliament to critically address the alleged need for data retention. Through proposals for the narrowing of this exception that would make data retention laws legally problematic under EU law, the European Parliament made itself a political actor in the debate about data retention, which had previously be beyond its reach since it was debated in the third pillar and at the national level. Thus, the need for inclusion of provisions delineating the scope of the e-Privacy Directive, allowed the European Parliament to assert power outside of its generally accepted field of competence.

Ultimately, the proponents of the possibility of data retention regimes at the national level prevailed in the negotiations at the EU level. The provision mandating the deletion of data after they had served their legitimate business purpose survived but an exception ensured there was space for the adoption of national data retention laws. More specifically, not long after 9/11 the Council and Parliament adopted the new e-Privacy Directive (2002/58) containing an exception to the obligation to delete meta-data with a specific reference to data retention instruments. Article 15, first paragraph of the Directive allowed Member States to "adopt legislative measures providing for the retention of data for a limited period" when this would constitute "a necessary, appropriate and proportionate measure within a democratic society" in view of the general goals including "national security (i.e. State security), defence,

[18] See e.g. Marc Richard, Senior Counselor for Criminal Justice Matters, DoJ, Prepared statement of the United States of America Presented at EU Forum on Cybercrime, Brussels, 27 November 2001, available at http://cryptome.org/eu-dataspy.htm. (Stating that "Because traffic data and mobile device location data are critical to apprehend terrorists and criminals and to prevent the execution of planned terrorist and criminal acts, the United States opposes mandatory data destruction regimes.").

public security, and the prevention, investigation, detection and prosecution of criminal offences."[19]

While this result allowed each European country to pursue data retention regimes nationally, the debate in the third pillar context on police and justice cooperation continued, controversially and mostly outside the reach of public scrutiny, and it became apparent that a significant number of Member States wanted to ensure European-wide mandatory data retention through a EU level instrument. After the Madrid bombings in 2004, the European Council made this a priority of its counter terrorism agenda,[20] and a Framework Decision for the mandatory retention of subscriber and traffic data across the EU was debated throughout 2004 and 2005. The European Parliament advised critically and against it, but had no legal powers to stop the Council.[21]

Then there was a significantly change of course in the way in which data retention was addressed at the EU level. While no agreement had yet been reached to adopt a framework decision in the Council, the position was put forward that data retention had to be regulated under the first pillar, since the resulting obligations on service providers would affect the single market for electronic communication services. As a result, the debate partly shifted back to the first pillar and the EC put forward a proposal for a European-wide harmonized data retention framework in September 2005, amending the existing e-Privacy Directive discussed above. In other words, data retention was now expressly considered as an internal market issue at the EU level.

The political consequences of this shift between the two pillars were significant. First, it gave the Parliament the power to amend the proposal and negotiate with the Council. Second, it meant that Member States no longer had a veto in the Council and therefore, a single Member State would not be able to obstruct the adoption of a Framework Decision.[22] In December 2005, the DRD was adopted under enormous political pressure on the European Parliament, just a few months after the EC had made its proposals. At the core of the DRD was a data retention regime mandating the storage for a period of 6-24 months of electronic communications traffic and location data, "in order to ensure that the data are available for

[19] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002, pp. 37 – 47, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

[20] The European Council, Declaration on Combating Terrorism, Brussels, Mar 25, 2004, http://consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.

[21] European Parliament, *Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, Brussels, May 31, 2005, (8958/2004 – C6-0198/2004 – 2004/0813(CNS)), Committee on Civil Liberties, Justice and Home Affairs, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//EN.

[22] It is worth noting that the Council only took the Framework Decision off its agenda when the adoption of the DRD was in sight.

the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law", with the possibility to mandate longer retention. The Directive gave no definition of serious crime and remained absolutely silent on the fact that intelligence agencies would be amongst the primary beneficiaries of the new regime. Most of the EC's original proposals for provisions directed at the safeguarding of the internal market did not make it into the final Directive.[23]

3.3. The Directive under Scrutiny by the CJEU

The CJEU has considered the legality of the DRD twice. First, in a 2009 judgment, after a challenge by Ireland and supported by Slovakia that it was based on the wrong legal basis.[24] Second, in 2014, after challenges by civil society in Ireland and in Austria, leading to prejudicial questions about the legality of the Directive in view of its impact on fundamental rights.[25] In its first judgment, the Court sanctioned the Directive's adoption as a first pillar internal market Directive.[26] In its second judgment, the Court annulled the Directive due on the basis of its interference with the fundamental rights to privacy and data protection.[27] More specifically, as will be discussed below, the Court concluded that the Directive did insufficiently consider the impact on the fundamental rights and the need to restrict this impact to the necessary minimum.

In its first judgment on challenge of the DRD's legal basis by Ireland, the Court accepted the reasoning of the European legislature that the DRD was in fact a proper internal market Directive, harmonizing data retention obligations to ensure the single market in electronic communications services. Its reasoning was based on two observations. First, it concluded that there were indeed legitimate reasons for the European legislature to be concerned about the internal market impact of diverging national approached to the question of data retention.[28] Second, it argued that "the provisions of Directive 2006/24 are designed to harmonise national laws on the obligation to retain data (Article 3), the categories of data to be retained (Article 5), the periods of retention of data (Article 6), data protection and data security (Article 7) and the conditions for data storage (Article 8)."[29]

This latter conclusion on the DRD's actual harmonization, is the least convincing part of the Court's judgment, considering the fact that no proper harmonization of any of these things resulted from the adoption of the Directive.[30] Under the DRD, the categories of data were the

---

[23] See European Commission, Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, {SEC(2005) 1131}, Brussels, Sep 21, 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:EN:PDF.
[24] CJEU 10 February 2009, C-301/06 (*Ireland v. EP and Council*).
[25] CJEU 8 April 2014, Joined Cases C-293/12 and 594/12 (*Digital Rights Ireland*).
[26] CJEU 10 February 2009, C-301/06 (*Ireland v. EP and Council*).
[27] CJEU 8 April 2014, Joined Cases C-293/12 and 594/12 (*Digital Rights Ireland*).
[28] CJEU 10 February 2009, C-301/06 (*Ireland v. EP and Council*), par. 65-72.
[29] Id., par. 81.
[30] See e.g. Van Hoboken, Case Note CJEU 10 February 2009 C-301/06 (Ireland v. EP and Council), Privacy & Informatie, 2009.

subject of minimum harmonization. Thus, Member States could adopt national data retention laws for more categories of data and other services, unrestricted by the DRD.[31] While such minimum harmonization is not uncommon in view of other regulatory aims, such as consumer protection, from an internal market perspective this does not make a lot of sense, since the service providers remain confronted with the possibility of divergent legal obligations. Furthermore, the period of retention between 6-24 months, and possibly longer under a special notification regime, could hardly be called harmonization.[32] Data security and the conditions of storage were only very generally stipulated. The cost reimbursement provisions proposed by the European Commission, which were of particular relevance to the industry, were not included in the final Directive.[33] Considering these deficiencies from an internal market perspective and the role of the European Commission as defender of the internal market, the European Commission's defense of the Directive's adoption in later policy discussions remains somewhat troubling.

Finally, the Court concluded that the Directive was based on the proper legal basis in the Treaties since its provisions were "essentially limited to the activities of service providers and do not govern access to data or the use thereof by the police or judicial authorities of the Member States."[34] In other words, the subject of regulation was the *availability of data in the private sector*, not the conditions under which access would take place in the Member States. Thus, the *separation* of availability from the reasons for keeping the relevant data available, i.e. access, provides the basis of the legality of the EU's approach to address data retention as an internal market issue.[35]

The separation between availability and access featured again in the Court's second judgment on the DRD in 2014, when it finally addressed the interference of mandatory blanket data retention with fundamental rights. The judgment is complex and its interpretation ongoing,[36] but for the purposes of this Article we can already make the following observations.

---

[31] From recital 12 in combination with Article 15 e-Privacy Directive it is clear that the data set in the DRD is a minimum. Many national implementations did in fact go beyond this minimum. See also EC, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, Apr. 18, 2011.

[32] Article 6 and Article 12, DRD. For an overview of the resulting choices, see EC, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, Apr. 18, 2011 (Concluding "that the Directive provides only limited legal certainty and foreseeability across the EU for operators operating in more than one Member State and for citizens whose communications data may be stored in different Member States.").

[33] See Article 10 of the European Commission Proposal, which stated that: "Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive." European Commission, Proposal, 2005. See also EC Staff Working Document, Extended Impact Assessment, Annex to the Proposal for a Data retention Directive, http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/sec/2005/1131/COM_SEC(2005)1131_EN.pdf.

[34] CJEU 10 February 2009, C-301/06 (Ireland v. EP and Council), par. 80.

[35] See also, Reidenberg, Forthcoming, at 103.

[36] While the UK has chosen to react to the annulment of the Directive with fast tracked new legislation, other Countries have seen opposite dynamics. For a discussion, see Boehm & Cole, Data Retention after the Judgement of the Court of Justice of the European Union, Muenster & Luxemburg, June 30th, 2014,

The Court concludes that the DRD constitutes a "particularly serious" and "wide-ranging" interference with the right to private life (Article 7 of the EU Charter) and the right to protection of personal data (Article 8).[37] In the Court's view, the interference does not concern the essence of the rights, since the DRD does not affect the communications content (Article 7) and still requires that services respect "certain principles of data protection and data security" (Article 8).[38]

The Court is satisfied that data retention satisfies an "objective of general interest". With a reference to Council's conclusions from 19 December 2002 that "data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime," it concludes that "the retention of data for the purpose of allowing the competent national authorities to have possible access to those data […] genuinely satisfies" this criterion.[39] With respect to the question of proportionality things get more complicated. The Court concludes that data retention will provide "the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations."[40] It does not agree with the argument that this is called into question by the possibility to circumvent data retention regimes, but it clarifies that the severity of the objective (to ensure public security) cannot by itself justify its adoption. [41]

The Court then proceeds to clarify the ways in which the DRD is not limited to what is strictly necessary from the objective pursued. It observes that the obligations cover "all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime" and critically notes the absence of exceptions in view of professions afforded with professional secrecy obligations and privileges.[42] Crucially, the Court notes that the DRD "does not require any relationship between the data whose retention is provided for and a threat to public security."[43] In other words, the retention of all data, because some of them could become useful is considered disproportional. The Court suggests that it would expect such a relation

---

http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf. The UK Data Retention and Investigatory Powers Act 2014 was adopted in July 2014. See http://services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers.html. For a very detailed overview of the implementation of the DRD, see the Country Reports of the Invodas Study, commissioned by the German government, http://www.emr-sb.de/gutachten-leser/items/forschungsprojekt-invodas-laenderberichte.html.

[37] Later in the judgment, the Court notes that the DRD "entails an interference with the fundamental rights of practically the entire European population." CJEU 8 April 2014, Joined Cases C-293/12 and 594/12 (*Digital Rights Ireland*), par. 56.

[38] Id., par. 40.

[39] Id., par. 44.

[40] Id., par. 49.

[41] Id., par. 51.

[42] Id., par. 57.

[43] Id., par. 59.

to the threats to public security "(i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences." [44] These considerations by the Court seem to imply that blanket data retention is, outside specific contexts, itself disproportional from a fundamental rights perspective.

Subsequently, the Court questions the proportionality of the DRD considering the absence of "any substantive and procedural conditions" relating to the access to the data retained by national authorities.[45] It notes that the retention period's necessity is questionable since it applies to all data without distinction and there are no objective standards stipulated on the basis of which the period should be set at the national level.

In the Court's final considerations about the lack of safeguards "against the risk of abuse and […] unlawful access and use of that data" it notes the lack of strict security requirements for the data collections created as a result of the DRD and the fact that the it "permits those providers in particular to have regard to economic considerations when determining the level of security which they apply."[46] And finally, in what could be considered an illustration of the impact of the Snowden revelations in Europe, it notes the absence of a requirement that "the data in question [are] to be retained within the European Union."[47]

3.4. Analysis

It is clear from this short history of data retention at the European level that institutional dynamics have been leading, throughout, and not the substance of the privacy issue to be regulated. Leading Member States, and in the background the United States, wanted to prevent 'data destruction' in the private sector for public sector reasons which they did not want to debate fully at the EU level. In effect, this blocked a fundamental debate about the relation between public sector demands and private sector data generating architectures. In particular, the separation of availability and access considerations made it impossible to have a proper European level debate about data retention and its proportionality.[48] This cannot be repaired by addressing this at the national level since the DRD created a new political reality in the Member States: after the adoption of the DRD, the general obligation to implement EU laws featured dominantly in discussions at the national level.

Perhaps the most striking is the absence of national security considerations or references to the access to the retained data by national intelligence agencies in the European debate and

[44] Id., par. 59.
[45] Id., par. 61.
[46] Id., par. 67.
[47] Id., par. 68.
[48] See also Reidenberg, forthcoming, at 113 (Noting that "data retention and access rules cannot be divorced from one another and the standards for linkage are elusive").

official documents related to data retention. This absence is a direct result from the lack of competency of the EU in national security matters and intelligence agency operations, a lack of competency well illustrated by the recent revelations about SIGINT operations of GCHQ in Brussels.[49] The legislative debate at the EU and its exclusion of national security, allows the EU to become a forum for the implicit covert regulation in view of national security demands in the Member States. In other words, secrecy is not only established at the level of execution of intelligence community powers, but also with respect to the regulation of the conditions for such execution as well.

The separation of availability from the reasons for keeping data available, i.e. access, provides the basis of the legality of the EU's approach to the data retention issue in the DRD, an approach that was validated by the CJEU in 2009 when it ruled on the DRD's legal basis. In its second ruling, however, the Court questioned the legality of the DRD, in view of the proportionality requirement following from Article 8 ECHR and Article 7 and 8 of the Charter, because of the lack of substantive and procedural conditions on access. With this conclusion, the Court de facto ensures that any future data retention instrument at the EU level would have to lead to harmonization of criminal procedural safeguards, which will be a difficult process for the Member States.

Clearly, the CJEU's approach fits with its traditional tendency towards the promotion and defense of European integration. In its first ruling, it protects the EU legislature to legislate on the basis of internal market considerations. In the CJEU's second ruling, it champions itself as the upholder of fundamental rights, which have become a central element of the EU narrative, and establishes criteria that have far-reaching consequences for the Member States.

Starting in the mid-1990s, the European Parliament kept struggling to have a say about the matter of data retention, discussed in the EU third pillar. When it succeeded to get a say in 2001 and in 2005, it did not make a subsequent impact. Under pressure, it adopted the space for national exceptions to the obligations on service providers to delete data in the ePrivacy Directive in 2001, and in 2005 it adopted the DRD uncritically. The European Commission has played a crucial role in the management of the data retention dossier at the EU level for more than a decade but its impact on the substance has been quite minimal. In particular, the European Commission was unsuccessful in shaping the DRD as a real internal market directive. The current challenge for the EC to come with any data retention proposal that would both satisfy the CJEU's strict criteria in view of the right to privacy, while still pleasing the Member States is substantial.

[49] See e.g. Richard Norton-Taylor, UK and US spy chiefs have some explaining to do, The Guardian, Jul. 1, 2013, http://www.theguardian.com/uk/defence-and-security-blog/2013/jul/01/gchq-nsa-eu. See also European Parliament, Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

4. Privacy and Reputational Harms in Search Media

4.1. The Privacy Problem

With the rise of the World Wide Web, conflicts about the protection of privacy and (personal) reputation in the new media abound.[50] The possibility of internet users to self-publish has been one cause for the proliferation of legally questionable content online. Blogs, micro-blogging and social media, in particular, make the Web into a platform to share, debate, and comment matters ranging from the mundane and social to the artistic and political. These practices can happen without users having to get legal advice or professional training about the extent to which their publication practices stay within generally accepted ethical and legal boundaries.

An additional reason for a sharp increase in potentially harmful material has been the process of digitization by organizations. The publication of public records and the digitization of archives and making them accessible in the online environment has become common practice for governmental and non-governmental actors. The implications of making things public on the Web, however, and the implications of keeping them online are not always fully and properly accounted for.

The existence of search media has given online publicity about individuals, i.e. the availability of material online resulting from the dynamics identified above, its sharper edge. Search media have harnessed digital full-text, image and video search technologies and deployed innovative approaches to indexing and ranking in ways that have put much of the Web's online publicly available content at our fingertips. Privacy and reputations are made and broken by publishers, still, but arguably the real game changers are search engines.[51] They provide an effective digital looking glass on what is publicly accessible and present results to sources in response to user queries. 'People search', which includes ego-search, can end up functioning as an online megaphone for online information related to people. It has been one of the very popular uses of search media from the start. 'Web People Search' is an important research topic the field of information retrieval.[52]

This new form of publicity online constituted by search results, which I will shortly refer to as 'search media publicity', has presented the legal system with a challenge to balance privacy

[50] For a discussion, see Daniel Solove, The Future of Reputation: Gossip, Rumor and Privacy on the Internet, Yale University Press, 2008. Clearly, reputation issues are prevalent in the business and government contexts also but this is outside the scope of this paper.
[51] As evident, for instance, from the focus on search by reputation management practices and services.
[52] See e.g. Nuray-Turan et al., Exploiting Web Querying for Web People Search, ACM 2012, http://www.ics.uci.edu/~dvk/CV/pub3.pdf. Since people's names are not unique, a core research challenge for Web People Search is disambiguation.

and reputation on the one hand and freedom of expression on the other hand. This challenge has involved the search for answers to the following range of interrelated questions:

- How should existing laws protecting privacy and reputation with respect to the media apply to much wider and more varied publication and dissemination practices on the Web, also in view of potential accessibility through search engines?
- When organizations are digitizing public records and paper-based media archives, which responsibilities exist, if any, to consider privacy and reputational harms through search engines?
- More specifically, and more controversially, to what extent should after a certain lapse of time certain measures be taken at the source with respect to publicly accessible material once lawfully published online?[53]
- What is the legal responsibility of the facilitators of online expressive activities such as discussion forums, microblogging sites and social media to manage the wider availability of materials published on their platforms?
- And finally, what is the responsibility of search engines and other entities who help users to find and link to information that is publicly available online?

Many of these questions have never really been properly addressed at the European legislative level until quite recently. To some extent, this is the result of a lack of competency and regulatory tradition of the EU in the field of substantive rules on media content. More specifically, privacy and reputation protection in the media context has generally been the competency of the Member States, while being the subject of fundamental rights safeguards established by the ECHR.[54]

Starting in 1998, the EU has issued a number of official recommendations with respect to the protection of minors and human dignity in the context of audiovisual media and the internet to promote the establishment of self- and co-regulatory frameworks with respect to internet publication practices and their respect for human dignity and the protection of minors.[55] These

[53] Notably, the interference with freedom of expression resulting from the absence of a time restraint on the possibility to take legal action against a publication was the subject of an ECHR challenge. See ECtHR 10 March 2009, Times v. United Kingdom.

[54] The ECHR case law consistently provides that an equal balance needs to be struck between freedom of expression on the one hand and the right to private life on the other hand. No hierarchy exists between these rights, neither right should take precedence of the other and it should not matter for the outcome whether the case was brought to the Court with reference to one right or the other. See e.g. ECtHR 7 February 2012, Application nos. 40660/08 and 60641/08 (Von Hannover v Germany (no. 2)).

[55] See Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, Official Journal L 270 of 7.10.1998, http://europa.eu/legislation_summaries/audiovisual_and_media/l24030b_en.htm.

Recommendations are quite general in character, however, and did not stipulate substantive legal rules on the lawfulness of publications in view of the protection of privacy and reputation.

The same is true for the existing (conditional) intermediary liability exemptions established by the Electronic Commerce Directive (ECD), which do not properly address or anticipate social networking sites or search media. Articles 12-15 ECD are applicable to the question of responsibility of access and hosting provider activities with respect to third party infringements of protections of privacy or reputation, but the question of what counts as an infringement is determined by the law of the Member States. Perhaps most remarkable is the absence of specific legislative activity and debate with respect to search engines at the EU level.[56] Even though the liability exemptions in the ECD were modelled after the DMCA, search engines were not included in the Directive and this was largely undebated too. The status of search engines in the Member States has diverged and under the ECD the status still remains somewhat unclear as a result of the confusing interpretations by the CJEU of the scope of Article 14 ECD.[57]

As will become apparent shortly, without this being the result of a deliberate decision by the EU legislature, it has been the European data privacy framework established in 1995 that has slowly and gradually become the dominant framework for dealing with the questions stipulated above, including the question about the balancing of privacy and freedom of expression in the search engine context. Data protection authorities have applied the data protection framework to many of the questions above and issued official advice on the interpretation of data protection in some of these questions through the Article 29 Working Party. Specific proposals for a right to be forgotten with reference to public personal data in the online environment and the problems of effective uncontrolled further dissemination feature centrally in the proposals for a Regulation.[58] Most recently, the CJEU established the legal responsibility of search engines as controllers under EU data protection rules for the personal data in their index and search results.[59]

---

[56] For a discussion, see e.g. 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. See also Van Hoboken, Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU, International Journal of Communications Law & Policy, No. 13, 2009.

[57] Id., at 246-259.

[58] 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; Reding, Privacy matters – Why the EU needs new personal data protection rules, Brussels, 30 November 2010; Reding, The future of data protection and transatlantic cooperation', Brussels, 6 December 2011; Reding, Your data, your rights: Safeguarding your privacy in a connected world', Brussels, 16 March 2011. In the same sense: Reding, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age', Munich, 22 January 2012. C, 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.

[59] Infra Section 4.5.

4.2. The Applicability of EU Data Protection Rules to Online Publishing

The omnibus character of the DPD in combination with its open norms and principles for fair and lawful processing of personal data ensures it can be applied flexibly across different sectors. This is typically argued to be one of the strengths of the European approach to data privacy issues, in Europe in particular, in contrast to the approach followed in the United States, where only specific sectors are subject to specific mandatory data privacy rules and the processing of person-related information in the private sector remains largely a matter of self-regulation and negotiated market practices subject to FTC oversight.[60]

Since the strict application of the DPD framework to the media was generally considered to be inconsistent with the protection of a free media and free press, the DPD did include a provision to ensure a balance with freedom of expression would be struck at the national level.[61]

> Article 9 Processing of personal data and freedom of expression
>
> Member States shall provide for exemptions or derogations from the provisions of this Chapter,[62] Chapter IV[63] and Chapter VI[64] 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.

The language of the provision and its reference to 'solely for journalistic purposes' has lent itself to a strict interpretation that only those activities that are functionally equivalent to journalism or amount to artistic or literary expression fall within its scope.[65]

The incompatibility of the full applicability of the DPD framework with freedom of expression could be the result of a variety of data protection rules and principles. First, the increased emphasis on consent as a legal basis for processing, the legal basis stipulated as the default rule in Article 8 of the Charter, is generally inconsistent with freedom of expression and a free media. Furthermore, the general prohibition of the processing of personal data such as data

---

[60] For a discussion, see e.g. Schwartz, EU-U.S. Privacy Collision, at 1973-1976. See also Bennett & Raab 2006, at 125-133.

[61] To a large extent, the existence of a media exemption in the DPD was also the result of similar exemptions in the national laws that the DPD was harmonizing. On the legislative history, see e.g David Erdos, Confused? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection, University of Oxford, Legal Research Paper Series, 2012/; David Erdos, From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection, August 8th, 2014, SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477797.

[62] General rules for lawful processing, strict rules for processing of special categories of data and data subject rights.

[63] Transfer to Third Countries.

[64] Supervisory Authority Provisions.

[65] The reason for the inclusion of the wording 'solely' was to make clear that the provision did not apply to non-journalistic data processing activities, such as the management of subscriber databases. For a discussion of the legislative history of Article 9, see Erdos 2012. See also Lee Bygrave, Data Protection Law: Approaching its Rationale, Logic and Limits, Information Law Series Nr. 10, Kluwer Law, 2002, at 55-56.

about someone's race and ethnicity or health would clearly be incompatible with freedom of expression.[66] The data subject rights to transparency and the right to gain access to one's personal data specifically, would make it possible for anyone fearing publicity to request access to one's data from investigative journalists. And the Data Protection Authorities could turn themselves into media oversight agencies and conduct investigations into the practices of journalists with respect to the sources of their reporting on individuals.[67]

Predictably, the implementation of the media exemption has varied considerably.[68] In some Member States, media are completely exempted from all the respective provisions. In others, such as in the Netherlands, an exemption is made for some of the rules, but the general rules on lawfulness of processing remain applicable.[69] Interestingly, the Article 29 Working Party debated the exemption in its first year of establishment in 1996[70] and adopted its first ever Recommendation on the issue in 1997.[71] While it does stipulate that "anybody [could be] processing data for journalistic purposes", the Recommendation is mostly informed by the concern that exemptions or derogations would be applied too broadly.[72]

Clearly, the problem of stipulating the proper exemptions and derogations for freedom of expression protected activities was a serious and complex task for the national legislatures. The main problem with Article 9 has been the scope of applicability itself. Due to the pervasive digitization in society and the structural changes of the media environment that involve many new players, the question about the scope of Article 9 has gained urgency over the years. Nowadays, there is hardly any freedom of expression protected activity that takes place through non-automated means and many of involve someone's personal data. The basic definitional structure and design of the DPD has the result that any private sector and non-household activity involving any type of processing of personal data, a concept which is defined notoriously broadly, is fully covered by the DPD rules unless it can invoke Article 9 protection. Thus, in its *Lindqvist* judgment in 2003 the ECJ concluded that "referring, on an internet page, to various persons and identifying them by name or by other means […] constitutes 'the processing of personal data wholly or partly by automatic means'".[73] The

[66] Reportedly, the Greek law requires media to get a permit to process sensitive data from the DPA, a problematic interference with freedom of expression. See Technical analysis of the transposition in the Member States, Annex to the First Report on the Transposition of the Data Protection Directive (16.05.2003), available at http://ec.europa.eu/justice/data-protection/document/transposition/index_en.htm.

[67] Notably, recital 37 DPD states that "at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities."

[68] For an overview by the EC, see Technical Annex to First Report on the Implementation of the DPD, at 17-19, available at http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

[69] Dutch Data Protection Act, Article 3(1).

[70] Article 29 Working Party, First Annual Report (1996), WP3, Brussels, 25 June 1997, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp3_en.pdf.

[71] Article 29 Working Party, Recommendation 1/97 on Data protection law and the media, WP1, Brussels, Feb 25, 1997, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp1_en.pdf.

[72] Id.

[73] CJEU 6 November 2003, C-101/01 (*Linqvist*), par. 27.

possible full applicability of Directive was not considered to be incompatible with freedom of expression, but the question whether Article 9 would apply and how freedom of expression would be accounted for was left to be determined at the national level.[74]

The question about the scope of Article 9 was further addressed, still in general terms, by the Court in its *Satamedia* judgment in 2008. The case involved an SMS service in Finland that allowed the public to gain access to publicly available tax records for a fee. The records were clearly public, they were also legally published in a Finnish newspaper. After its launch, the service was confronted with an enforcement action by the Finnish Data Protection Ombudsman to cease this activity.[75]

In appeal the case led to questions about the scope of Article 9 to the CJEU, which established that the media exemption must be interpreted broadly: Article 9 does not only apply to media undertakings, but to "every person" engaged in journalistic activities.[76] In addition, journalism should not be understood in a narrow 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."[77] This interpretation has received quite some criticism for its broadness and disregard for more nuanced interpretations in the Member States and the case law of the ECHR.[78] National courts, including the Finnish Court after the ruling have found ways to impose some further conditions for the media regime to apply, such as the requirement that the disclosure should be directed at the public as a communal entity, be directed at an issue of public concern, or that there should be some editorial activity involved.[79]

Notably, the Court's AG Kokott had clearly advised the Court to "follow the cautious line" in proscribing a precise interpretation of how to balance freedom of expression in the data protection framework.[80] She had argued, that "the Court, when striking a balance between conflicting fundamental rights in the context of the Directive, should in principle allow the Member States and their courts a broad discretion within which their own traditions and social values can be applied."[81]

4.3. Search Media Publicity under the DPD

The impact of search media on the right to private life and data protection did not go unnoticed in international data protection circles. In 2006, the International Data Protection and Privacy

[74] An important first case arose in Sweden. For commentary see Lee Bygrave, Balancing data protection and freedom of expression in the context of website publishing - recent Swedish case law, Privacy Law and Policy Reporter, 2001, http://www.austlii.edu.au/au/journals/PrivLawPRpr/2001/40.html#fnb8.
[75] CJEU 16 December 2008, C-73/07 (*Satamedia*), par. 25-31.
[76] Id., par. 58.
[77] Id., par. 61 and 62.
[78] See e.g. Anne Flanagan, Defining 'journalism' in the age of evolving social media: a questionable EU legal test, International Journal of Law and Information Technology, 2012.
[79] See Erdos 2012.
[80] CJEU, Opinion of AG Kokott of 8 May 2008, C-73/07 (*Satamedia*), at 50.
[81] Id., at 53.

Commissioners' Conference adopted a resolution on "Privacy Protection and Search Engines", which expresses concerns about the data privacy issues related to the collection and processing of detailed user data, search queries in particular.[82] Notably, the Resolution explicitly did not address "the issues raised by the practice of many search engines to store and publish copies of the content of websites, including personal data published on such sites legally or illegally."[83]

Subsequently, the Article 29 Working Party addressed the application of the DPD to the processing of personal data in the search engine context, including the question about the applicability to issues raised by People Search.[84] The Working Party discerned two main processing activities, namely the processing of user data on the one hand, and the processing of content data on the other hand. With respect to the processing of user data, i.e. search engine logs, it noted the supporting role of data protection to protect freedom of expression of search engine users. Freedom of expression is served by the application of data protection rules ensuring the fair proportionate and transparent processing of search engine logs. With respect to such user data it provided for a detailed interpretation of the obligations of the search engines as the controller with respect to their processing.[85] With respect to the latter, i.e. the personal data in the index and search results, it the Article 29 Working Party it proceeded more carefully and noted 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 data on the one hand and the free flow of information and the fundamental right to freedom of expression on the other hand."[86]

More specifically, the Article 29 Working Party tried to delineate the responsibility of search media under data protection rules for the personal data in search results through a cautious interpretation of the controller concept. It asserted that the primary controllers of personal data in the index of a search engine were those responsible for the publication of this data on the Web.[87] Moreover, it noted that the legal responsibility of intermediaries such as search engines to remove personal data depended on the law in the Member States, including other laws as data protection laws determining the legality of publications about people infringing their privacy or harming their reputation.[88] An exception, in the Working Party's view, existed

[82] See 28th International Data Protection and Privacy Commissioners' Conference London, Resolution on Privacy Protection and Search Engines, United Kingdom, 2-3 November 2006, http://privacyconference2011.org/htmls/adoptedResolutions/2006_London/2006_L4.pdf.
[83] Id.
[84] See Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, Brussels, Apr 4, 2008, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.
[85] The enforcement actions of European DPAs, led by the French CNIL, against Google in Europe with respect to its changes of its privacy policy in 2012 trace back to the user data parts of the opinion on search engines. See most recently, CNIL, The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc., Jan 8 2014, http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/
[86] Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, at 13.
[87] Id., at 14.
[88] Id.

in the case of the caching copies by search engines containing personal data, if these data were no longer available on the Web itself, as well as in the case of value-added operations on the personal data specifically.[89] But generally, it concluded that "when it comes to the content data, search engine providers are generally not to be held primarily responsible under European data protection law."[90]

While most European DPAs followed the Working Party line that search engines should generally not be considered responsible under data protection rules for the personal data in their index, the Spanish DPA, AEPD, continued its enforcement actions with respect to search engines. In particular, the AEPD put forward the view that "the initial incorporation of […] personal information on the web may be legitimate at source, its universal and secular conservation on the Internet may be disproportionate".[91] Even more strikingly, the AEPD was of the view that even in situations in which Spanish law required the data to be maintained public at the source, data protection law still provided for a remedy at the search engine. In one specific case, the AEPD requested the deletion of a link from the search engine to a public announcement in the media of the public auction of the property of a Spanish citizen, Mario Costeja González.[92] Google disagreed, leading to the CJEU's *Google Spain* judgment that has been widely reported on from the earliest stages and I typically considered as an example of the 'right to be forgotten'.[93]

The legal proceedings between the AEPD and Google took place against the background of the debate about the proposals for a new Data Protection Regulation, proposed by the European

---

[89] Id.

[90] Id., at 23.

[91] See Spanish Data Protection Agency (AEPD), Statement on Internet Search Engines, Dec. 1 , 2007, at 10, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/statement_aepd_search_engines_/Statement_AEPD_Search_Engines_en.pdf. Notably, the AEPD's conclusion that data subject rights to request the erasure of data on the basis of data protection law, was partly based on the Spanish Law implementing the safe harbor for information location tools, established in the implementation of the ECD. Thus, the AEPD turned the safe harbor against the search engines, by interpreting the condition for a safe harbor into an actual legal obligation.

[92] See Audiencia Nacional, *Google Spain v. AEPD*, 2012, http://www.poderjudicial.es/search/doAction?action=contentpdf&reference=6292979&publicinterface=true.

[93] See Van Hoboken 2012, at 254-255; Van Alsenoy et al., Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?, 2013; Josh Halliday, 'Google to Fight Spanish Privacy Battle', The Guardian, January 16, 2011, http://www.guardian.co.uk/technology/2011/jan/16/google-courtspain-Privacy; Josh Halliday, 'Europe's highest court to rule on Google privacy battle in Spain', The Guardian, Mar. 1, 2011, http://www.guardian.co.uk/technology/2011/mar/01/google-spain-privacy-court-case; M. Peguera, 'Spain asks the ECJ whether Google must delete links to personal data', Mar 2, 2012,: http://ispliability.wordpress.com/2012/03/02/spanish-court-asks-the-ecj-whether-google-must-delete-links-to-personal-data/; M. Peguera, 'Google Spain wins lawsuit over the "right to be forgotten"', 27 February 2012, http://ispliability.wordpress.com/2012/02/27/google-spain-wins-lawsuit-over-the-right-to-be-forgotten/; Franz Werro, 'The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash', in: A.C. Ciacchi, et al. (eds.), Liability in the Third Millennium, Baden-Baden, F.R.G., 2009; Peter Fleischer, 'The right to be Forgotten'', seen from Spain, Sept. 5, 2011, http://peterfleischer.blogspot.com/2011/09/right-to-be-forgotten-seenfrom-spain.html; The Guardian, http://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth.

Commission in 2012.[94] A central element in the EC's proposals was a more explicitly stated and strengthened right for data subjects to request erasure of their personal data as well as the abstention from their further dissemination, stipulated in Article 17 of the proposal. In the view of the EC, the right to be forgotten was needed to meet one of the main challenges for the protection of privacy, i.e. the need to give data subjects more control over their data.

4.4. The Proposed Regulation, the Right to Be Forgotten and Freedom of Expression

The legal proceedings between the AEPD and Google took place against the background of the debate about the proposals for a new Data Protection Regulation, proposed by the European Commission in 2012.[95] A central element in the EC's proposals was a more explicitly stated and strengthened right for data subjects to request erasure of their personal data as well as the abstention from their further dissemination, stipulated in Article 17 of the proposal. In the view of the EC, the right to be forgotten was needed to meet one of the main challenges for the protection of privacy, i.e. the need to give data subjects more control over their data. As will become clear below, these proposals also entailed the potential regulation of search engine publicity at the EU level through the use of data protection laws.

The right to be forgotten as proposed by the European Commission and publicly defended by EC Vice-President Viviane Reding could be considered quite a political success. Newspapers around the world received the proposals by explaining how in Europe people would be granted the right to have their data deleted.[96] The popularity of such a proposal should have come as no surprise to the Commission. An official survey of privacy attitudes amongst the European public had concluded that "[a]s regards the "right to be forgotten", a clear majority of Europeans (75 %) want to delete personal information on a website whenever they decide to do so".[97]

The right to be forgotten has been one of the most hotly debated topics in scholarship related to the data protection review.[98] Without doing justice to all the nuances of this debate it is

---

[94] For a detailed analysis of the EC's proposal from the perspective of freedom of expression, see Van Hoboken 2013.

[95] For a detailed analysis of the EC's proposal from the perspective of freedom of expression, see Van Hoboken 2013.

[96] See e.g. Somini, Sengupta, Europe Weighs Tough Law on Online Privacy, NYTimes, Jan.24, 2012; Stanley Pignal, Companies face big fines in plan to bolster EU data protection, FT, Dec 5. 2011; Park Si-soo, 'Right to be forgotten' matters in Internet Age, Korea Times, Feb 15, 2012; Julian Swallow, Facebook and Google spark privacy fears, The Advertiser (Australia), Jan. 27, 2012. See 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 (Stating in the headline: "EU-citizens may make their data disappear from the Internet").

[97] See Special Eurobarometer, 359, Attitudes on Data Protection and Electronic Identity in the European Union, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[98] See e.g. Meg Ambrose & Jef Ausloos, The Right to be Forgotten Across the Pond, Journal of Information Policy 3, 2013, p. 1-23; Meg Ambrose, It's About Time: Privacy, Information Lifecycles, and the Right to be Forgotten." Stanford Technology Law Review 16, 2013, at 369-422; Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88, 2012, http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten; J. Ausloos,

worth taking a look at some specific details of the proposal. Remarkably, when looking at the EC proposals for the right to be forgotten from January 2012 carefully, arguably, there is no such thing as an actual new right to get data deleted in the new Article 17.[99] The proposal adds a lot of text but doesn't add that much substantively in comparison to the current DPD framework. The situations in which erasure or the abstention of further dissemination of personal data would have to be granted by the controller depend on the rules of the legitimate grounds for processing and the interpretation of rules on purpose limitation. If the basic principles for the fair and lawful processing of personal data are not strengthened in the Regulation, there is no ground to speak of an actual new 'right' to be forgotten or erasure. In fact, there may be more reason to conclude the contrary. Some of the proposals that have been tabled to introduce a special regime for pseudonymous data could seriously undercut any data subject rights with respect to data processed about them by industry and government entities, including rights to access data as well has rights to have them deleted.[100]

While in earlier proposals that were leaked, Article 17(2) made reference to services such as search engines, the new elements with respect to public information in Article 17(2) of the EC final proposal are likely to be inconsequential. They merely contain a duty to inform in the case the controller has 'authorized' a third party publication. Still, in light of the question about the application of data protection to public processing of personal data, the stipulation of a special rule with additional obligations in view of personal data made public in view of the consequences for the individual is notable. Also notable is the specific reference in the text about the erasure of links and references in publicly available communication services which are still present in the text of Article 17(9)(b) and give the EC a power to interpret rules about the deletion of links, copies or replications of personal data in such services.[101] The regulation of the dissemination of personal data through search engines therefore appear to remain part of the ambit of the Proposed Regulation.

Both the Council and the European Parliament have developed positions that would amend Article 17 as proposed by the EC considerably. The European Parliament compromise amendments, adopted in March 2014, remove the 'right to be forgotten' from the text of the Regulation but seem to strengthen the right to erasure in some respects. The right to have

---

'The 'Right to be Forgotten' – Worth Remembering?', Forthcoming Computer Law & Security Review, 2012; P.S. Castellano, 'The right to be forgotten under European Law: a Constitutional debate', Lex Electronica vol. 16.1, 2012, at 1-30; E.J. Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice', SCRIPTed, 2012, at 229-256; 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, at 67-72;

[99] See also, Joris van Hoboken, The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Research Paper Prepared for the European Commission, May 2013, http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf.

[100] For instance, the proposals that would give a de facto legitimate interest for the processing of pseudonymous personal data, i.e. personal data kept separate by the controller from identifiers.

[101] This text is still present in the EP amended version as well, even though the reference is now unclear after the Parliament's amendment of Article 17(2) of the Regulation.

links, copies or replication of data deleted has been more clearly stipulated and has been included in Article 17(1) along an additional ground to obtain the right to erasure, namely in case "a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased".[102] The EP's Article 17(2) provides that if the data were made public without a legal justification in the data protection framework (such as consent, a legal obligation or a legitimate interest which included freedom to expression), the controller should take reasonable steps to obtain deletion of the data, including by third parties, and inform the data subjects of the relevant actions taken by such third parties, to the extent possible. The Council's position on the proposals is still developing. Council working documents made public in May 2013 show that it has developed a complete overhaul of Article 17 and the Council document lists a long list of reservations, questions and arguments against specific elements of the original proposal for Article 17.[103]

What the debate about a new Regulation hasn't done is resolve the question about the status of search engines under the rules for the processing of personal data in their index and search results. In the EC proposals, 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 engines could still be considered controllers of the personal data in their index. For instance, the safe harbors in Directive 2000/31/EC still leave room for injunctions and administrative orders.

The new proposals for a freedom of expression exemption in Article 80 remain almost as vague about the scope and which exceptions and derogations are necessary as Article 9 DPD is currently. It is instructive to consider the results of the EP's first reading on Article 80 and recital 121. The resulting Article 80(1) provides that:

> Member States shall provide for exemptions or derogations from the provisions [in Chapter II, III, IV, V, VI, VII, and specific data processing operations in Chapter IX] whenever this is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression in accordance with the Charter of Fundamental Rights of the European Union.[104]

---

[102] Compromise Amendments on Articles 1-29, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf; It is unclear to the author what is precisely meant with this wording. The amendment has no clarification.

[103] 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.

[104] Compromise Amendments on Articles 30-91, Proposal for a regulation of the European Parliament and of

This is generally in line with the need to acknowledge freedom of expression protected activities outside of journalism. But the complete lack of guidance on the types of exceptions and derogations is striking. The listed Chapters cover everything, except for Chapter I on definitions and general material and territorial scope, Chapter VIII on legal remedies and Chapter X which contains a specific provision for EC rulemaking.[105] Therefore, it is not clear what the value of this specification of Chapters is. At best it is a vague signal that it is not allowed to exempt covered activities completely but more likely it is a mere symbolic act of guidance to the Member States. The room and lack of specific guidance given to the Member States is particularly problematic considering the growing importance of the scope and implications of Article 80. It is also a very poor fit with the choice for a Regulation instead of a Directive.

Additionally, Article 80 seems to have been written with publishers (in the broad sense) in mind and does not address the question of how to apply Article 80 to entities that help these publishers find a way to an audience, such as search engines. Recital 121 as amended by the EP provides that:

> it is necessary to interpret notions relating to [..] freedom [of expression] broadly to cover all activities which aim at the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them, also taking into account technological development.[106]

All in all, the hot potato is passed to the Member States. This makes any claim by the EU legislature that it has balanced data protection with freedom of expression properly questionable.

4.5. The CJEU in Google Spain

In light of the ongoing debate about a new right to be forgotten in the new Regulation, it came as some surprise that the CJEU used the opportunity of the proceeding between AEPD and Google to discover a right to be forgotten in the existing data protection framework. The judgment has led to a flood of reactions in the media, not the least of them in the United States.[107] In a far-reaching judgment on the interplay between data protection and freedom

---

the
Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

[105] The impact of the exclusion of these Chapters, for instance the Chapter on Remedies will of course greatly depend on the precise derogations and exceptions provided for in the Member States.

[106] Compromise Amendments on Articles 30-91.

[107] See e.g. Danny Sullivan, http://searchengineland.com/eu-right-forgotten-191604; AP, European court: Google must yield on personal info, http://www.washingtonpost.com/world/europe/european-court-google-must-amend-some-results/2014/05/13/f372fe08-da78-11e3-a837-8835df6c12c4_story.html; Jonathan Zittrain, http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0, Charles Arthur,

of expression at the EU level, the Court answers the question whether search engines could be obligated to remove links in response to people search queries on request of the relevant data subjects.[108] The Court concludes that Google is the controller for the processing of personal data in its index and search results, and concludes that these processing operations fall within the territorial scope of the DPD.[109]

The Court was apparently not convinced by the more cautious approach by the Working Party and the Court's AG of the question about the controller status. The latter had emphasized the right to freedom of expression and had also advised the Court that search engines should be considered processors, i.e. entities that process data but have more limited responsibilities under data protection law.[110] In the Court's view, however, the requirement of "effective and complete protection of data subjects" implies that search engines have to be considered controllers, even though they do "not exercise control over the personal data published on the web pages of third parties".[111] This "effective and complete protection" requirement appears to be new in European fundamental rights jurisprudence.[112] Five times in total, the Court uses this *deus ex machina* to strike down arguments to be cautious about the full application of

---

http://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth. David Lee, http://www.bbc.com/news/technology-27407017; Lily Hay Newman, http://www.slate.com/blogs/future_tense/2014/05/13/right_to_be_forgotten_european_court_rules_google_has_to_remove_search_results.html?wpisrc=burger_bar; Daniel Solove, What Google Must Forget: The EU Ruling on the Right to Be Forgotten, LinkedIn, Influencer, May 13, 2014, https://www.linkedin.com/today/post/article/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten (Noting in particular that "In the EU, there is great concern over articulating first principles – a broad statement of fundamental rights.), Hayley Tsukayama, http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/13/right-to-be-forgotten-highlights-sharp-divide-on-u-s-european-attitudes-toward-privacy/. Eric Posner, http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html. NYTimes, http://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?hp&rref=opinion. Aarti Shahani, http://www.npr.org/blogs/alltechconsidered/2014/05/16/313021079/european-ruling-on-removing-google-links-may-leave-a-mess. Henry Farrell and Abraham Newman, Forget Me Not: What the EU's New Internet Privacy Ruling Means for the United States, Foreign Affairs, May 19, 2014, http://www.foreignaffairs.com/articles/141435/henry-farrell-and-abraham-newman/forget-me-not#cid=soc-twitter-at-snapshot-forget_me_not-000000. Evan Selinger and Woodrow Harzog, http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/; Jef Ausloos, European Court Rules against Google, in Favour of Right to be Forgotten, LSE Media Policy Project, May 13, 2014, http://blogs.lse.ac.uk/mediapolicyproject/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/.

[108] CJEU 13 May 2014, C-131/12 (*Google Spain*), at 89-99.

[109] As some commentators have noted, the Court has not clarified if its ruling extends to processing in google.com or only through google.es, the service directed at Spain. See Jonathan Zittrain, Is the EU compelling Google to become about.me?, The Future of the Internet, May 13, 2014, http://blogs.law.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/.

[110] See Opinion of AG Jääskinen, CJEU 13 May 2014, C-131/12 (*Google Spain*).

[111] CJEU 13 May 2014, C-131/12 (*Google Spain*), at 34.

[112] Normally, the requirement is that the protection of fundamental rights should be "practical and effective" and not "theoretical and illusory". See e.g. ECtHR 11 July 2002, *Goodwin v. the United Kingdom*, par. 74.

data protection responsibility to search engines, territorial overreach and data subject rights.[113]

The conclusions on Google's controller status were not the most surprising. It is on the need to balance with the right to freedom of expression that the Court's judgment goes awry.[114] While the AG discusses the need to balance with freedom of expression, i.e. the freedom to receive and impart information and ideas as protected by Article 11 of the Charter and Article 10 ECHR at length, the Court does not even refer to Article 11 explicitly. Most striking is the consideration of the Court that the privacy rights of data subjects to request their information to be removed from search engines

> "override, *as a rule*, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name".[115]

Outside of this default rule and a consideration with respect to the role played by the data subject in public life, the Court does not give search providers (or the national Data Protection Authorities charged with oversight) much legal guidance on the question of how to balance data protection with the right of the public to inform itself when deciding what to do in response to a request. The Court does add that "it is not necessary in order to find such a right [to prevent specific people search results from appearing] that the inclusion of the information in question in the list of results causes prejudice to the data subject."[116] The data does not necessarily have to be "inaccurate".[117] "[T]he fact that they are inadequate, irrelevant or excessive in relation to the purpose of processing" could be enough.[118] Fundamentally, the Court does not consider the extent to which its ruling encroaches on the fundamental right to freedom of expression of Web users. It also does not seem or want to realize that search engines may invoke the right to freedom of expression themselves, for instance to offer a search engine on the Web and refer users to lawful and publicly available material online.[119]

Finally, the Court's considerations about the scope of Article 9 DPD are perplexing in view of its earlier *Satamedia* ruling. With a return of a reference to 'solely for journalistic purposes' it seems to overrule its earlier broad interpretation. Specifically, in the Google Spain case it considers that the publication on a web page of personal data "may, in some circumstances be carried out 'solely for journalistic purposes' and thus benefit from derogations" based on Article 9. In the Court's view, however, "that does not appear to be so in the case of the

---

[113] CJEU 13 May 2014, C-131/12 (Google Spain), par. 34, 38, 53, 58 and 84.
[114] See also Steve Peers, The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression, EU Law Analysis, May 13, 2014, http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html.
[115] CJEU 13 May 2014, C-131/12 (Google Spain), at 97 (emphasis added).
[116] Id., at 96.
[117] Id., at 92.
[118] Id., at 92.
[119] For a detailed study of the implications of the right to freedom of expression in the search engine context, see Van Hoboken 2012.

processing carried out by the operator of a search engine."[120] The Court gives no arguments for this conclusion. Notably, this conclusion may be deliberately vague, in view of divergent views on the matter in the Members States and leaves room to national DPAs and Courts to conclude otherwise.[121]

Thus the Court opens the doors for data subject requests to have personal data removed from search engines widely. The conclusion is simply that search engines process data in their index and search results on the basis of Article 7(f) DPD, which requires a balancing between the interests pursued by the controller, those to whom the data are disclosed against the interests of the data subject. Data subjects have rights to have personal data corrected and deleted and can object to the processing of their data in individual cases.

4.6. Analysis

The way search engine publicity issues have been dealt with in Europe over the last two decades provides a fascinating and somewhat disturbing perspective on the development of the European approach to privacy that is the subject of this Article. More specifically, it shows how the data protection framework has slowly and relatively quietly, i.e. without significant debate amongst legal scholars or policy makers, become the legal instrument to regulate privacy and reputational harms in the networked public information environment. A rough way to summarize this paradigmatic shift for a U.S. audience is that the publication and further dissemination to the public of publicly accessible information related to individuals, including the media in a broad sense of the word, would become regulated by a stricter version of the Fair Information Practice Principles (FIPPs), subject to oversight by the FTC.

Arguably, this is a major legal paradigmatic shift with significant consequences for the publication and dissemination of information to the public and the appreciation of freedom of expression interests, consequences that have started to materialize very clearly with the *Google Spain* judgment. European legal systems have traditionally relied on different and much older legal doctrines, such as privacy and reputational torts, the protection of dignity, press and media law, as well as the fundamental rights jurisprudence of the ECHR with respect to the balancing of the right to private life and the right to freedom of expression since the 1950s. In other words, doctrines developed over time in the cultural-legal traditions of the member states, informed by different attitudes to privacy and reputational issues in the media, which have until now not been harmonized, except very generally through the general fundamental rights jurisprudence of the ECtHR in case-specific instances. The new paradigm, instead, involves the application of a legal instrument, data protection, developed since the 1960s in response to the emerging use of ICTs for personal record management practices of

[120] CJEU 13 May 2014, C-131/12 (Google Spain), at 85. This wording appears to be less ambiguous in the original language of the ruling. See also Kulk and Zuiderveen, Google Spain v. Gonzáles: did the Court forget about freedom of expression?, European Journal of Risk Regulation, Forthcoming 2014.

[121] See James Fontanella-Khan, Data protection agencies gain power from Google defeat, FT.com, May 14th, 2014, http://www.ft.com/intl/cms/s/0/157eecaa-db82-11e3-b112-00144feabdc0.html.

government bodies and industry. Thus, existing doctrines are replaced with a European-wide doctrine that establishes ex ante mandatory rules for the handling of information, has primarily been concerned with the production of transparency over the management of personal records by such organizations and involves a system of public oversight by, (in the book) independent, government agencies staffed with data privacy specialists.

A crucial question for the medium to long term is whether this development is a stable one. Is correction still possible and feasible, in view of the problematic implications for the protection of freedom of expression? Or is this in fact the European approach to privacy and reputation issues related to different forms of publicity in the online environment? In current legal terms and on the short term, the answer to this question resolves around the interpretation of Article 9 DPD and the likely adoption of a new Article 80 in the Regulation. Clearly, these provisions do not establish much legal certainty and the amount of fundamental debate about these provisions relative to debate about other aspects of the Regulation is not promising for those who'd like to see more guidance on the way to ensure respect for freedom of expression in the context of the application of data protection rules. This makes it highly likely that the CJEU will have a significant future role in providing further legal guidance on the question of how to balance freedom of expression in the data protection context. Unfortunately, its suboptimal jurisprudence about the scope of Article 9 are not very promising in this respect.

To conclude this section it is worth exploring certain features in the European environment that have made this shift possible. First, as noted in the beginning of the Section, the European approach is an omnibus approach to data privacy issues, which is without doubt also one of its strengths. With respect to the media environment, including new kinds of media and services for the dissemination of publicly available information, the difficulty of drawing a line has made it possible for data protection to erode other legal doctrines. The omnibus logic appears hostile to exceptions and informs an approach that all data processing practices should be covered for data protection to be effective. In Google Spain, the CJEU goes as far as using a new criterion that protection should be "effective and complete". Thus, data protection is displacing other legal approaches to resolving privacy and reputational harms. In fact, most of the time, there seems to be no realization that there exist in fact other, perhaps more appropriate doctrines that could be applied to these complex issues. Furthermore, proponents of strict enforcement of data protection, for instance to the processing of user data by search engines, welcome strict application of data protection to search engine publicity also, since they do not seem to recognize the necessity to differentiate between the different problems the legal system is presented with.[122]

While these are dynamics related to the substance of privacy laws, it is clear that there are significant institutional dynamics at play as well, similar as in the case of data retention. To

[122] See e.g. Rik Ferguson, Counterpoint: "Right to be forgotten" is the step in the right direction, Index on Censorship, May 21, 2014, http://www.indexoncensorship.org/2014/05/counterpoint-right-forgotten-step-right-direction/. ("Enshrining the right to be forgotten is a further step towards allowing individuals to take control of their own data […]").

start with, there are the DPAs overseeing the compliance with the omnibus approach to data privacy issues. This oversight involves receiving complaints by the public about the infringement of privacy. Considering the urgency which unpleasant, harmful, unlawful, or simply annoying online publicity can have for those affected and the fact that those complaining will not necessarily be informed about the boundaries of data protection in the media context, a significant number of complaints about privacy and reputational harms in online media arrive at the national DPAs. Thus, there is an incentive for DPAs to enforce on issues that may be outside of data privacy in the strict sense. The fact that the CJEU's judgment in Google Spain has established the full legitimacy of DPA enforcement of complaints with respect to search engines means that DPAs have less of a reason to be cautious if they do not see a reason to. As the President of CNIL explains to Le Monde, a third of the complaints they receive is about a right to be forgotten with respect to information available online:

> "Cette décision est assez symbolique et fait écho à une demande sociale qui s'exprime de façon insistante : le nombre de plaintes relatives au droit à l'oubli que l'on nous adresse a explosé, cela représente un tiers de nos plaintes."[123]

At the EU level, the European Commission has deliberately incorporated privacy and reputational harms into their proposals for a new Regulation and a right to be forgotten in particular. Regardless of some of the sharp criticism in response, making these privacy issues part of the debate has in many ways been a significant political success and granted much more visibility to the proposals. The promises with respect to more control over publicly available data, without properly explaining the precise consequences of its proposals for relevant contexts or the extent to which control over personal data would not always be legally appropriate, seems to come closest to a form of privacy populism. Above all, the EC has done a rather dubious job of relating data protection to the existing approaches to protecting privacy and reputation in the Member States discussed above. From the perspective of the EC, it may simply be attractive to largely replace national legal doctrines with one general Regulation: displacing other privacy laws with data protection implies that the EC's competency is growing.

The CJEU, finally, has championed its typically European integrationist approach on the one hand and its more recent role as arbiter of fundamental rights issues at the highest instance on the other hand. Its approach in Google Spain still needs to be digested further but it seems clear that it finds itself ever more comfortable to significantly shape the contours of privacy doctrine in Europe.

5. Transnational Surveillance of the Cloud.[124]

[123] Alexandre Léchenet et Martin Untersinger, 'Isabelle Falque-Pierrotin : "Je ne crois pas du tout à la fin de la vie privée", Le Monde, May 19, 2014, http://www.lemonde.fr/technologies/article/2014/05/19/isabelle-falque-pierrotin-je-ne-crois-pas-du-tout-a-la-fin-de-la-vie-privee_4420923_651865.html.

[124] For background, see Van Hoboken, Arnbak and Van Eijk, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad, Jun 9, 2013, SSRN,

6. Conclusion

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.