The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines

Christopher Kuner

LSE Law, Society and Economy Working Papers 3/2015
London School of Economics and Political Science
Law Department

The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines

Christopher Kuner*

Abstract: In Case C-131/12 *Google Spain v. AEPD and Mario Costeja Gonzalez*, issued on 13 May 2014, the Court of Justice of the European Union recognized a right under the EU Data Protection Directive 95/46 for individuals to suppress links generated by Internet search engines (popularly referred to as the 'right to be forgotten'). The Court's holdings leave many important questions open, both in regard to technical legal issues and more high-level issues of general jurisprudential and societal importance. The judgment suffers from the Court's traditionally minimalist style of argument and reluctance to adopt a more open and discursive style, and its failure to take the significance of the case for the Internet into account. The material and territorial scope of the right to suppression must be defined in a way that is proportionate to the ability to implement it, if the judgment is to effectively protect fundamental rights in practice.

* Director, Brussels Privacy Hub, Vrije Universiteit Brussel (VUB); Visiting Fellow, Department of Law, London School of Economics; Affiliated Lecturer, University of Cambridge. This article is written in the author's personal capacity. The author is grateful for the valuable input of Hielke Hijmans, Julia Powles, and various European data protection officials who shall remain nameless. This paper is current as of September 2014. All website referred to in this paper have been last accessed in February 2015. A later version of this paper will be published in Studies of the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law, Nomos/Brill 2015.

I. INTRODUCTION

On 13 May 2014, the Court of Justice of the European Union (CJEU) issued a judgment of great significance for data protection law, EU fundamental rights law, and the Internet. In Case C-131/12 *Google Spain v. AEPD and Mario Costeja Gonzalez*,[1] the Court made several important pronouncements about EU data protection law, and in particular recognized a right under the EU Data Protection Directive 95/46 for individuals to suppress links generated by Internet search engines (popularly referred to as the 'right to be forgotten').

The judgment has probably been the subject of more academic commentary in a few months than other CJEU data protection cases have been in the 16 years since the Directive came into force.[2] It has received a wide range of reactions, from being hailed as a 'constitutional moment' resulting in a significant extension of fundamental rights in the EU,[3] to 'the most important right you've never heard of',[4] to a violation of the fundamental principle of freedom of expression,[5] to 'preposterous'[6] and 'deeply immoral'.[7] It has also been the subject of squabbles between polemicists in the EU and the US.[8]

The judgment is significant for its analysis of issues such as whether an Internet search engine should be considered to be a data controller or a data processor; the territorial application of EU data protection law; and the extension of data protection rights to the Internet. It also illustrates the stronger legal protection for fundamental rights since the entry into force on 1 December 2009 of the Lisbon Treaty,[9] which explicitly grants individuals a right to data protection

---

[1] The judgment is available at <http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065>.

[2] See the website <http://www.cambridge-code.org/googlespain.html>, listing dozens of academic blog entries on the case in the few months since it was issued.

[3] Indra Spieker genannt Döhmann and M. Steinbels, 'Der EuGH erfindet sich gerade neu', 14 May 2014, <http://www.verfassungsblog.de/der-eugh-erfindet-sich-gerade-neu/#.U_mOj7ySy-U>.

[4] Eric Posner, 'We All Have the Right to be Forgotten', 14 May 2014, <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>.

[5] See 'Index Blasts EU Court Ruling on the 'Right to be Forgotten", 13 May 2014, <http://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten/>.

[6] Stewart Baker, 'Contest! Hacking the Right to be Forgotten', 7 June 2014, <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/07/contest-hacking-the-right-to-be-forgotten/>.

[7] Sophie Curtis and Alice Philipson, 'Wikipedia Founder: EU's Right to be Forgotten is 'Deeply Immoral", 6 August 2014, <http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html>.

[8] Compare, for example, Joe McNamee, 'Google's Right to be Forgotten—Industrial Scale Misinformation?', 9 June 2014, <http://edri.org/forgotten/>, with Craig A. Newman, "A Right to be Forgotten' will Cost Europe', 26 May 2014, <http://www.washingtonpost.com/opinions/a-right-to-be-forgotten-will-cost-europe/2014/05/26/93bb0e8c-e131-11e3-9743-bb9b59cde7b9_story.html>.

[9] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, [2007] OJ C306/1. See also Orla Lynskey, 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order', 63 *International and Comparative Law Quarterly* 569 (2014).

in the Treaty on the Functioning of the European Union (TFEU)[10] and gives full legal effect to the EU Charter of Fundamental Rights.[11] The judgment provides one of the first indications of how the Lisbon framework affects the online sphere, and also represents a kind of 'test run' for many of the rights contained in the EU's proposed General Data Protection Regulation.[12]

Thus far, many commentators on the judgment have tended to praise or condemn it based on their own philosophical and political views. This article will instead analyze the legal issues that led the Court to its decision, and examine their implications for data protection, EU law, and the Internet.

After giving a brief description of the facts in the case, it will describe how the Court's holdings leave many important questions open, in regard to both technical legal issues and more high-level issues of jurisprudential and societal importance. The judgment also does not take the significance of the case for the Internet into account, and suffers from the Court's traditionally minimalist style of argument. The material and territorial scope of the right to suppress Internet search engine results are potentially much wider than the ability to implement the right effectively, which exemplifies the tendency in EU data protection law to impose wide-ranging obligations on data processing with little regard to how they can be enforced. This suggests that a way must be found to define the scope of the right to suppression in a way that is proportionate to the ability to enforce and implement it, if it is to provide real protection in practice.

II. THE JUDGMENT

The facts of the case, and the holding of the Court, can be briefly described based on the judgment and the opinion of Advocate General Jääskinen that preceded it.[13]

The plaintiff in the case, Mr. Costeja González, was mentioned in two announcements published in a Spanish newspaper dealing with attachment proceedings in a real estate auction prompted by social security debts. The newspaper had originally published the announcements in 1998, as required by Spanish law. At a later date, an online version of the newspaper became available, so that the announcements became accessible via a Google search. The plaintiff complained in 2009 to the newspaper seeking removal of the announcements

---

[10] Consolidated version of the Treaty on the Functioning of the European Union (TFEU), [2010] OJ C83/47, Article 16(1).

[11] Consolidated version of the Treaty on European Union (TEU), [2008] OJ C115/13, Article 6. See Charter of Fundamental Rights of the European Union, [2010] OJ C83/2, Article 8.

[12] 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.

[13] Case C-131/12, Opinion of Advocate General Jääskinen, 25 June 2013, <http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN>.

from the online edition, contending that the attachment proceedings were over and that the announcements were thus no longer of any relevance. The newspaper refused, as it said it was legally obliged to publish them. He also complained to Google Spain SL, seeking deletion of references to the announcements in the results produced by the Google search engine.[14] In response, Google passed the request on to Google Inc. in the US, stating that the latter entity was the operator of the search service.

The plaintiff then complained to the Spanish Data Protection Agency (DPA) against the newspaper and both Google entities, claiming that the newspaper should be required to take measures so that his personal data did not appear, and that Google should ensure that they did not appear in results produced by its search engines. On 30 July 2010, the Spanish DPA rejected the complaint against the newspaper, finding that it had a legal obligation to publish the information under an order of the Spanish Ministry of Labour and Social Affairs. However, the DPA upheld the complaints against both Google entities, and ordered them to take measures so that the complainant's data no longer appeared in Google search results. The two Google entities then appealed the DPA's decision to the Spanish Audiencia Nacional (National High Court), which stayed the actions and referred the following questions to the CJEU for a preliminary ruling (quoted here in edited form from para. 20 of the judgment):

> 1. With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:
> (a) must it be considered that an 'establishment', within the meaning of Article 4(1)(a) of Directive 95/46, exists […] when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State […]
>
> 2. As regards the activity of search engines as providers of content in relation to Directive 95/46 […]:
> (a) in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of 'processing of […] data' used in Article 2(b) of Directive 95/46?
> (b) If the answer to the foregoing question is affirmative, and once again in

[14] It is unclear from the judgment and from the Advocate General's opinion exactly which search domains were covered by the complaints (i.e., whether they included the main Google search engine google.com, the Spanish Google search engine google.es, or both; see par. 43 of the judgment).

> relation to an activity like the one described: must Article 2(d) of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the 'controller' of the personal data contained in the web pages that it indexes?
>
> 3. Regarding the scope of the right of erasure and/or the right to object, in relation to the 'derecho al olvido' (the 'right to be forgotten'), the following question is asked: must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?'

On June 25, 2013, Advocate General Jääskinen issued his opinion in the case and answered the three main questions posed as follows (in para. 138 of his Opinion):

> 1. Processing of personal data is carried out in the context of the activities of an 'establishment' of the controller within the meaning of Article 4(1)(a) of the EU Data Protection Directive 95/46/EC 'when the undertaking providing the internet search engine sets up in a Member State, for the purposes of promoting and selling advertising space on the search engine, an office or subsidiary which orientates its activity towards the inhabitants of that State.'
>
> 2. An internet search engine service provider that located information published by third party web sites 'processes' personal data in the sense of Article 2(b) of Directive 95/46 when that information contains personal data. However, it should not be considered a 'controller' of the data processing in the sense of Article 2(d) of the Directive as long as it does not index or archive personal data against the instructions of the web page's publisher.
>
> 3. The rights provided by the Directive (and in particular the rights to erasure and blocking of data provided for in Article 12(b), and the right to object provided for in Article 14(a)) do not confer to an individual a right to prevent a search engine service provider from indexing the information relating to him that is published legally on third parties' web pages.

In its judgment, published on 13 May 2014, the Court held as follows (see para. 100):

--The activity of an Internet search engine in finding information placed on the Internet by third parties, indexing it, storing it, and making it available in a particular order of preference constitutes data processing. However, in contrast to the Opinion of the Advocate General, the CJEU found that the operator of a search engine is to be considered a data controller rather than a data processor. This is because the operator determines the purposes and means of data processing by the search engine (para. 33), and because the objective of the relevant provisions of the Directive is to ensure effective and complete protect of data subjects through a broad definition of the concept of 'controller' (para. 34). The Court determined that Google Inc. is both the actual operator (para. 43, second bullet) and the data controller (para. 60) of the Google search engine.

--The processing of personal data by a search engine that is operated by an undertaking established outside of the EU but that has an establishment in the EU is carried out 'in the context of the activities' of such establishment within the meaning of Article 4(1)(a) of the Directive, if such establishment promotes and sells advertising space in such Member State that serves to make the search engine profitable (para. 55), thus leading to the application of EU data protection law. This is so because the activities of the local establishments are 'inextricably linked' to the activities of the Google headquarters in the US since their activities allow the search engine to be economically viable (para. 56). In this respect, EU data protection law should be interpreted to be given a 'particularly broad territorial scope' in order to prevent individuals being deprived of the protection of the Directive and of such protection being circumvented (paragraph 54).

--Articles 12(b) and 14(a) of the Directive should be interpreted to mean that an individual has a right to have a search engine remove links to web pages published by third parties from search results that are made on the basis of a search on a person's name. This right applies regardless of whether the material indexed is removed from such third party web pages themselves, and regardless of whether it was posted lawfully (paragraphs 62-99).

--Exercise of this right must respect a 'fair balance' between the fundamental rights of individuals to delete links and the interest of others in having access to such information (paragraph 81). The rights of the individual should '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', though the individual's rights should not take precedence if other factors would justify an

interference with them, such as the data subject's role in public life (paragraph 97).

III. LEGAL ISSUES RAISED BY THE JUDGMENT

Three legal issues raised by the judgment are particularly significant, namely its material scope; its territorial scope; and the threshold for invoking the rights affirmed by the CJEU. As discussed below, the answer to each of these questions is unclear.

A. MATERIAL SCOPE

Confusion has been created by widespread reports in the media that the CJEU created a new 'right to be forgotten' allowing individuals to have information about them deleted from the Internet.[15] The judgment and the opinion of the Advocate General have contributed to this confusion by their use of the term: the Advocate General stated that the case involved the question of whether to recognize the right to be forgotten (para. 6 of his opinion), and while the Court did not use the term in its rulings (para. 100), it did refer to it in the judgment (see paras. 20 and 91).

In fact, the judgment does not create a right to be forgotten. A careful reading shows that the right affirmed by the Court is that of obliging the operators of Internet search engines to suppress links to web pages from the list of search results made on the basis of a person's name (see para. 100), not a right to have data itself deleted from the Internet. Indeed, search engines could not themselves delete information from the web sites that they index, since these reside on servers hosted by other parties. For this reason, the right will be referred to herein as the 'right to suppression' of links to search engine results. This right is based on the Directive's Article 12(b) (covering the right to rectify, erase or block data) and Article 14(a) (covering right to object to data processing) of the Directive (see para. 82).

The questions referred to the Court concern 'Internet search engines', a term which the Court defines as 'a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference' (para. 21). However, this definition raises questions. Providers of Internet search engines, such as Google,

---

[15] See, e.g., Foo Yung Chee, 'Europe's Top Court: People Have Right to be Forgotten on Internet', 13 May 2014, <http://www.reuters.com/article/2014/05/13/eu-google-dataprotection-idUSL6N0NZ23Q20140513>, stating that 'The case underlines the battle between advocates of free expression and supporters of privacy rights, who say people should have the 'right to be forgotten' meaning that they should be able to remove their digital traces from the Internet'.

Bing (i.e., Microsoft), Yahoo etc. are obviously covered.[16] But countless other Internet services provide large-scale search functionality (e.g., social networks, Internet archives, news databases etc.) and many web sites other than search engines have a search function embedded in them. It may also be questioned whether the judgment should be limited to services that are accessible to all Internet users; for example, many information services are accessible via the Internet and include a search functionality (e.g., commercial news databases), but may be used only with a password or other access limitation. While access to these services is limited, they may still have millions of users.

The popular perception seems to be that the judgment concerns a few large Internet search engines, but if one views the Court as taking a functional approach to the definition of the services covered, the question becomes whether a principled distinction between Internet search engines and other Internet sites with large-scale search functionality (including commercial databases) can be made such that the judgment would not apply to the latter. From the author's point of view, such a distinction is not obvious, particularly in view of the fact that the judgment is based so strongly on the protection of fundamental rights. In particular, the Court refers to the objective of the Data Protection Directive 95/46 'of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data', and adds that 'those words cannot be interpreted restrictively' (para. 53). Thus, it seems that the material scope of judgment should be broadly interpreted to extend beyond particular Internet search engines to also cover a wide variety of online services that provide search functionality on a large scale.

The scope of searches covered by the judgment is also unclear. The Court's ruling covers 'a search made on the basis of a person's name' (para. 100), but the third question referred to the Court concerning the suppression of search engine results refers instead to 'indexing of the information relating to him personally' (para. 20), though the summary of the facts by the Court seems to indicate that the complainant was concerned about searches made on his name (para. 14). One could argue that the plaintiff had only complained about searches on his name, and thus there was no need for the Court to consider other types of searches. However, research has demonstrated that individuals can easily be identified by searching for data fields other than their name,[17] and given the Court's emphasis on the protection of fundamental rights, it seems difficult to argue that the scope

[16] See Press Release, 'European DPAs meet with search engines on the 'right to be forgotten'', 25 July 2014, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf>, describing a meeting the Article Working Party had with Google, Microsoft, and Yahoo.

[17] See Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', 57 *UCLA Law Review* 1701, 1705 (2010), citing a study stating that a search using postal code, date of birth, and sex allows the identification of 87% of people in the US.

of the search terms covered should be limited to names, if this would result in a gap in protection.

B. TERRITORIAL SCOPE

The relevant issues concerning the judgment's territorial scope can be divided into two categories, namely first of all the intra-EU application of data protection law (i.e., determining which EU Member State's law applies to the processing), and second, the application of EU data protection law to data processing outside the EU.

With regard to the first set of issues, the CJEU applied EU data protection law (and thus Spanish law) to Google Spain based on Article 4(1)(a) of the Directive, i.e., on the basis that data processing by the Google search engine is carried out in the context of the activities of Google Spain as an establishment of Google Inc. The two crucial assumptions underlying this conclusion are that, first, Google Inc. is a data controller, and second, that the Google search engine processes data in the context of the activities of Google Spain. The first assumption (that Google Inc. is a data controller) directly contradicts the Advocate General, who had found that an Internet search engine is not a data controller with regard to the personal data on source web pages hosted on third party servers (paras. 89-90 of his Opinion). However, the Court found that the definition of 'data controller' should be broadly construed, in order to provide 'effective and complete protection of data subjects' (para. 34). This conclusion has broad implications, as many web services seem to operate on an assumption that they are 'data processors', and are not subject to the full panoply of data protection compliance obligations that apply to controllers under the Directive.

In its conclusion that the Google search engine is a data controller, the Court did not engage with the arguments made by the Advocate General that the concept of a data controller in the context of the Internet requires it to 'apply a rule of reason, in other words, the principle of proportionality, in interpreting the scope of the Directive in order to avoid unreasonable and excessive legal consequences' (para. 30 of the Advocate General's opinion). The Court also could have built on its statement that 'the operator of the search engine as the controller in respect of that processing must ensure, *within the framework of its responsibilities, powers and capabilities* [emphasis added], that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect' (para. 83). That is, the Court could have indicated that even if a search engine that processes information put on the Internet by a countless number of parties around the world is to be considered a data controller, the level of compliance responsibilities it has should be judged within its possibilities for exercising them, and that these possibilities may be different than is the case with many other types of data controllers.

With regard to the second assumption (that search engine data are processed in the context of the activities of Google Spain), many DPAs have long reached a

similar conclusion in cases where an EU-based establishment is closely involved in data processing that is carried out by its non-EU parent company. The author wrote as early as 2003 that 'in many cases Member State DPAs will be quite imaginative in finding that there is some sort of connection between the processing and the establishment' of a company in a Member State, and that this may lead to the entity being considered to be 'established' in such Member State for data protection purposes.[18] However, the CJEU's statement that the economic support provided by Google Spain for the Google search engine (i.e., the support provided for the Google group's advertising activity) results in it being 'inextricably linked' with the operation of the search engine by Google Inc. is the most authoritative confirmation yet that an EU-based subsidiary of a multinational company with headquarters in another region may be subject to EU data protection law even if it doesn't actually operate the data processing service at issue. This conclusion is based largely on the strengthening of the fundamental right to data protection under the Lisbon framework (see para. 58 of the judgment). It also confirms that each EU establishment of a non-EU based data controller is subject to the national law of its respective Member State of establishment. Further clarification of the intra-EU application of national data protection laws under the Directive will come when the CJEU issues its judgment in the pending *Weltimmo* case.[19]

The second set of issues (application of EU data protection law outside the EU) is of perhaps more wide-ranging importance. The Court did not deal with the application of EU data protection law to processing by data controllers established outside the EU under Article 4(1)(c) of the Directive (see para. 61), since it found that EU data protection law applies to Google Spain under Article 4(1)(a) and thus was able to sidestep consideration of whether Article 4(1)(c) should apply.[20] Despite the fact that the data controller (Google Inc.) is located outside the EU, and the service at issue (the Google search engine) is accessible around the world via the Internet, the Court failed to say anything concerning the case's implications for non-EU data controllers, and virtually nothing about its potential impact on

---

[18] See Christopher Kuner, *European Data Privacy Law and Online Business* (OUP 2003), at 95, stating that is the case under Finnish and Swedish law, for example.

[19] Case C-230/14 Weltimmo, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=154887&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7662>. In this case, which was referred to the CJEU on 12 May 2014 by a Hungarian court, the questions referred include the following one: 'Can Article 4(1)(a) of the data protection directive, read in conjunction with recitals 18 to 20 of its preamble and Articles 1(2) and 28(1) thereof, be interpreted as meaning that the Hungarian Data Protection and Freedom of Information Authority (a Magyar Adatvédelmi és Információszabadság Hatóság, 'the data protection authority') may not apply the Hungarian law on data protection, as national law, to an operator of a property dealing website established only in another Member State, even if it also advertises Hungarian property whose owners transfer the data relating to such property probably from Hungarian territory to a facility (server) for data storage and data processing belonging to the operator of the website?'

[20] The Court raised the question of the applicability of EU law under Article 4(1)(c) in para. 44, but stated in para. 61 that there was no need to examine this question further.

the Internet.[21] This is particularly striking since in its only previous case dealing with data protection on the Internet, the Court held that the Directive should not be interpreted so as to be applicable to the entire Internet.[22] The judgment affirms a right to have search engine results suppressed under certain circumstances, but gives no indication of the territorial scope of the right, and does not address the extent to which the right applies outside the EU.

The Court did not limit assertion of the right to suppression to EU individuals, or to search engines operated under specific domains. An individual seeking to assert a right under the Directive need not be a citizen of an EU Member State,[23] or satisfy any other jurisdictional requirements under private international law,[24] as long as the act of data processing on which his or her claim is based is subject to EU data protection law under Article 4. Thus, the judgment seems to place no territorial limits on application of the right, so that it could apply to requests for suppression from individuals anywhere in the world.[25]

For example, it seems that under the judgment there would be no reason why a Chinese citizen in China who uses a US-based Internet search engine with a subsidiary in the EU could not assert the right affirmed in the judgment against the EU subsidiary with regard to results generated by the search engine.[26] Since only the US entity running the search engine would have the power to amend the search results, in effect the Chinese individual would be using EU data protection law as a vehicle to bring a claim against the US entity. The judgment therefore potentially applies EU data protection law to the entire Internet, a situation that was not foreseen when the Directive was enacted.[27] This could lead to forum shopping and 'right to suppression tourism' by individuals with no connection to the EU other than the fact that they use Internet services that are also accessible there. Even if the judgment is likely to be interpreted in practice more restrictively

---

[21] The only such mention occurs in para. 81, stating that 'the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information […]'

[22] Case C-101/01 Bodil Lindqvist [2003] ECR I-12971, at para. 69.

[23] See Directive 95/46, Recital 2, stating that it applies 'whatever the nationality or residence of natural persons […]' See also Christopher Kuner, 'Foreign Nationals and Data Protection Law: A Transatlantic Analysis', in: *Data Protection 2014: How to Restore Trust* 213 (Hielke Hijmans and Herke Kranenbourg eds.) (intersentia 2014).

[24] See Article 29 Working Party, 'Working document on determining the application of EU data protection law to personal data processing on the Internet by non-EU based websites' (WP 56, 30 May 2002), at 6; Lokke Moerel, *Binding Corporate Rules* (OUP 2012), at 152.

[25] See, e.g., Stewart Baker, 'Inside Europe's Censorship Machinery', *Washington Post*, 8 September 2014, <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/08/inside-europes-censorship-machinery/>, presenting a case in which Google apparently considered a suppression request from an American citizen based in the US. For further discussion of the territorial scope of the judgment, see Christopher Kuner, 'The right to be forgotten and the global reach of EU data protection law', *Concurring Opinions*, 1 June 2014, <http://www.concurringopinions.com/archives/2014/06/the-right-to-be-forgotten-and-the-global-reach-of-eu-data-protection-law.html>.

[26] Article 3(2) of the proposed EU General Data Protection Regulation (n 12) would limit the possibility of asserting the right to be forgotten by individuals without any connection to the EU, since the application of EU data protection law would be limited to 'data subjects residing in the Union'.

[27] See Bodil Lindqvist (n 22), paras. 68-70.

than this,[28] such broad application cannot be excluded based on the wording of the judgment.

EU data protection law is to be construed broadly in order to protect against its circumvention,[29] but there must be some limits to its territorial application, if it is not to be universally applicable to the entire Internet. It is thus important not only to affirm when the fundamental right of data protection applies to the Internet, but also to determine when it *does not* apply. As Milanovic states:

> the positive obligation of a state to ensure the human rights of persons within its jurisdiction from violations by private parties is not absolute, as states are neither omniscient nor omnipotent. What they must do is to exercise due diligence, i.e. to take all measures reasonably within their power in order to prevent violations of human rights.[30]

Legislation and case law in both EU Member States and third countries have been used to limit jurisdiction when a controversy or the parties do not have sufficient connection to the forum (e.g., with regard to libel tourism in the UK[31] and foreign tort claims in the US[32]), and similar action may be needed to limit the right to suppression.

C. CONDITIONS FOR EXERCISE OF THE RIGHT

Individuals, companies operating web sites, and data protection regulators need to know the conditions under which the right to suppress search engine results can be exercised, and what limitations exist on it. The judgment is less than clear in this regard.

It seems that the threshold for invoking the right is low, so that it may be applied in a wide variety of situations involving search results. This conclusion is supported by the emphasis the CJEU put on the individual's fundamental rights guaranteed by the Charter (para. 97). Some DPAs have indicated that to the extent they become involved in cases involving assertion of the right, they will focus on

---

[28] See David Smith [author's note: Deputy UK Information Commissioner and Director of Data Protection], 'Four things we've learned from the Google judgment', 20 May 2014, <http://iconewsblog.wordpress.com/2014/05/20/four-things-weve-learned-from-the-eu-google-judgment/>, stating that the ICO will focus on 'concerns linked to clear evidence of damage and distress to individuals' in enforcing the right.

[29] See para. 54 of the judgment, indicating the policy of the Directive against the circumvention of EU data protection law. See also Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013), chapter 5.

[30] Marko Milanovic, *Extraterritorial Application of Human Rights Treaties* (OUP 2011), at 210.

[31] See the UK Defamation Act 2013, section 9(2), which limits the jurisdiction of the UK courts in certain defamation cases unless England or Wales 'are clearly the most appropriate place in which to bring an action […]'

[32] See Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659 (2013), in which the US Supreme Court limited application of the US Alien Tort Claims Act with regard to actions taking place outside the US.

ones where there is 'clear evidence of damage and distress to individuals'.[33] While such prioritization is understandable from a practical standpoint, the ability of DPAs to limit the judgment to such situations seems legally doubtful, as the Court remarked that the right applies regardless of whether inclusion of an individual's name in search results 'causes prejudice' (para. 96).

The Court addressed the crucial issue of what the legal basis is under the Directive for data processing by Internet search engines, stating that 'under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f)' (para. 73), which requires a balancing of the opposing rights and interests of data subjects and data controllers (para. 74). In this regard, the Court makes it clear that the individual's data protection and privacy rights under Articles 7 and 8 of the EU Charter of Fundamental Rights generally outweigh the economic interests of the search engine operator and the rights of Internet users in using a search engine to locate information (para. 97). However, the Court also states that suppression may be refused in specific cases, based on a balancing test that considers factors such as 'the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, […] [and on] the role played by the data subject in public life' (para 81).

It seems that the Court expects the right to suppression to be implemented in a way that allows individuals to exercise it easily, quickly, and effectively.[34] This suggests that there should be a presumption that the right will apply by default in most cases, and that it should be enforced quickly by the data controller. The Court does recognize that there are other important interests competing with the right to suppression, but the wording and tone of the judgment makes it clear that instances in which the individual's assertion of the right to suppression are overridden by other interests are to be regarded as exceptional.[35] The Court mentions 'the important role played by the Internet and search engines in modern society' (para. 80) only in the context of the risk to develop a detailed profile of an individual, rather than with regard to the societal benefits that the Internet brings. The Court also gives little assistance in determining those cases in which the right to suppression should be overridden, besides listing the three criteria mentioned above in para. 81.

The judgment conflates the concepts of privacy and data protection, in that it makes assertion of the right to suppression dependent on factors such as the sensitivity of the data for the individual's private life and his or her role in public life that are closely related to the protection of private life (i.e., privacy), rather

---

[33] Smith (n 28).

[34] See, e.g., para. 84 of the judgment, rejecting the possibility of requiring individuals first to obtain erasure of information relating to them from the publishers of web sites, since if this were required, 'given the ease with which information published on a website can be replicated on other sites and the fact that persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved […]'

[35] See, e.g., para. 81.

than just control over the processing of personal data (i.e., data protection). Indeed, the Court states that search engines are likely 'to affect significantly the fundamental rights to privacy and to the protection of personal data' (para. 80), so that the judgment continues a trend in which the CJEU considers privacy-related issues as central to its decisions on data protection.[36]

IV. HIGH-LEVEL ISSUES

Taking a step back from the technical legal issues, the judgment also raises a number of important jurisprudential, philosophical, and societal ones.

A. STYLE OF THE JUDGMENT

The primary task of the Court was to answer the questions referred to it by the Spanish Audiencia Nacional. However, within this mandate, the Court has some flexibility to use a style of judgment that fits the case, based on factors such as the precision of the questions referred to it, whether the Court has already ruled on the points in question, and the extent to which questions of fact or of national law still have to be determined.[37]

The case has obvious international implications, because the data controller of the search engine is located outside the EU, as are many of the web sites hosting material that are indexed by search engines, and because the Internet by its nature allows global access to information. Thus, the Court could have provided some discussion of the case's importance for global communication on the Internet. However, the international aspects of the case are barely mentioned at all by the CJEU, and then only in the sections describing the facts of the case (for example para. 43), not in the legal discussion. This is in contrast to the opinion of the Advocate General,[38] and to the Court's 2003 *Lindqvist* judgment,[39] which both contain discussion of the impact of the relevant legal issues on the Internet. The judgment instead focuses almost completely on interpretation of the relevant provisions of the Data Protection Directive, the Charter of Fundamental Rights, and the case law of the CJEU, i.e., on EU law.

---

[36] See Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', 3 *International Data Privacy Law* 222 (2013), at 223, stating that 'the jurisprudence has justifiably considered privacy to be at the core of data protection'; Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in: *Reinventing data protection?* (Serge Gurthwirth, Yves Poullet, Paul De Hert, J. Nouwt, and Cecile de Terwagne eds.) 3 (Springer Science 2009).

[37] See Koen Lenaerts, 'How the ECJ Thinks: A Study on Judicial Legitimacy', 36 *Fordham International Law Journal* 1302, 1344-45 (2013).

[38] See, for example, paras. 25-31.

[39] See, for example, paras. 62-71.

While it would exceed the scope of this article to consider in detail the working style of the Court, its minimalistic, detached style of judgment is a regular feature of the CJEU's jurisprudence. The Court's style has been variously described by scholars of EU law as 'self-referential and detached',[40] 'overly abstract, vague, and elliptical',[41] and 'cryptic […] [and] Cartesian'.[42] The Court apparently limits on purpose its arguments to 'the very essential', and builds up its argumentative discourse 'progressively, i.e., 'stone-by-stone''.[43] The reluctance of the Court to cite or draw on materials from outside the EU has also been criticized.[44] Thus, anyone expecting that the significance of the case for data protection on the Internet would inspire the Court to adopt a more discursive style in the manner of the European Court of Human Rights, the German *Bundesverfassungsgericht* (Federal Constitutional Court), or the US Supreme Court was bound to be disappointed, which may play a role in some of the criticism the judgment has received.

Advocate General Jääskinen recognized the importance of the case for the global Internet and the need to strike 'a correct, reasonable and proportionate balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and internet users at large' (paragraph 31 of his opinion), but the Court seemed disinterested in these factors.[45] For example, the Court based its decision on the special data protection risks posed by Internet search engines (paragraphs 36-38 and 80), and thus established in effect a different regime for application of the right to suppression in the online world than applies offline. The judgment would have benefited in this regard from reference to comparative and international legal materials dealing with the protection of fundamental rights on the Internet, such as the resolution of the UN Human Rights Council of 29 June 2012 finding that the rights to freedom of expression and to cross-border communication must apply in both the online and offline worlds.[46]

---

[40] Gráinne de Búrca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?', 20 *Maastricht Journal of European and Comparative Law* 168, 184 (2013).

[41] Vlad Perju, 'Reason and Authority in the European Court of Justice', 49 *Virginia Journal of International Law* 307, 310 (2009).

[42] Joseph Weiler, 'The Judicial Après Nice', in: *The European Court of Justice* (Gráinne de Búrca and J.H.H. Weiler eds.) 215, 224 (OUP 2001).

[43] Lenaerts (n 37), at 1351.

[44] de Búrca (n 40), at 173, referring to 'a remarkable lack of reference on the part of the Court of Justice to other relevant sources of human rights law and jurisprudence'.

[45] See, e.g., para. 81, stating with regard to the seriousness of the interference with data protection and privacy rights at stake in the case, 'it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing'.

[46] UN General Assembly, Human Rights Council, 'The Promotion, Protection, and Enjoyment of Human Rights on the Internet', Doc. No. A/HRC/20/L.13, 29 June 2012, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc>. The Human Rights Council has itself emphasized the importance of EU human rights standards conforming to UN standards. See UN High Commissioner for Human Rights, 'The European Union and International Human Rights Law', <http://www.europe.ohchr.org/Documents/Publications/EU_and_International_Law.pdf>, at 8.

Questions with regard to the different treatment of online and offline data processing also arise with regard to the DPA's dismissal of the claim against the newspaper. The Court noted that the case against the newspaper was dismissed because its publication of the information complained about was authorized by an order of the Spanish Ministry of Labour and Social Affairs (para. 16). However, it seems that publication in the printed newspaper appeared in 1998 but the online publication occurred later (see para. 5 of the Advocate General's opinion). Given that in 1998 online newspaper archives did not exist on a large scale, the ministerial order could hardly have had them in mind when it was issued. Moreover, although the date the order was issued is not given, it must have dated from long before the Lisbon framework, and thus could not have taken into account the increased value given to data protection since the framework came into force. While the question of whether the right to suppression should apply to the newspaper was not before the Court, the importance of the case for striking a balance between the fundamental rights to data protection and freedom of expression called for a more detailed explanation of the legal status of the order of the Spanish Ministry and why it resulted in the newspaper being exempted from application of the right.

The Court could also have mentioned in this regard the decision of the European Court of Human Rights in *Times Newspapers Ltd. v. UK*, where the Court found that Internet news archives fall within Article 10 of the European Convention on Human Rights protecting freedom of expression, stating:

> In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10.[47]

However, the judgment does not even mention in its reasoning the European Convention on Human Rights or the jurisprudence of the European Court of Human Rights.

The role of the CJEU is changing, and its audience and visibility are broadening.[48] As the attention given to the judgment has shown, a major decision of the CJEU dealing with the Internet receives worldwide publicity. The judgment implied that the Court is aware that it will result in EU law applying to non-EU data controllers that are not subject to the enforcement jurisdiction of the EU

[47] Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), nos. 3002/03 and 23676/03, § 27, 10 March 2009.
[48] See Perju (n 41); J.H.H. Weiler, *The Constitution of Europe* (CUP 2005), at 212-214.

courts and DPAs,[49] in which case it must have an interest in bolstering the international acceptance of its rulings. The Article 29 Working Party has also recognized that the extraterritorial application of EU data protection law may serve to persuade non-EU data controllers to comply with EU data protection law, even when it may not be possible to enforce the law against them.[50] Mentioning the international implications of the judgment would only have increased the respect given to it by the international community.[51] Especially in cases involving an international communications medium like the Internet, the Court must avoid 'withdrawing into one's own constitutional cocoon, isolating the international context and deciding the case exclusively by reference to internal constitutional precepts'.[52]

B. NEED FOR FURTHER INFORMATION ABOUT THE SCOPE OF THE PROBLEM

We need more information about the requests to exercise the right to suppression that are being made and how they are being dealt with in order to determine how the right should best be implemented. Only when there is a sufficient body of reliable information about the scope of the issues created by the judgment will it be possible to decide what steps should be taken to deal with them.

Google has stated that as of 18 July 20014, it had received over 91,000 requests for suppression involving over 328,000 URLs,[53] which seems like a huge number considering that the judgment was handed down a little over two months

---

[49] See para. 84, stating 'Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.'

[50] Article 29 Working Party, 'Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites' (WP 56, 30 May 2002), at 15, stating that even if EU data protection law cannot be enforced in third countries, 'there exist examples that the foreign web site may nevertheless follow the judgment and adapt its data processing with a view to developing good business practice and to maintaining a good commercial image'. See also Dan Jerker B. Svantesson, 'The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on US Business', 50 *Stanford Journal of International Law* 53 (2014), arguing that jurisdictional claims under EU data protection law that cannot be enforced but that signal 'a perceived right to regulate a particular matter while acknowledging the lack of ability to regulate that matter' can still serve a useful function.

[51] See de Búrca (n 40), at 171, who states that overcoming its reluctance to consider and refer to legal standards outside the EU 'would provide the Court of Justice with relevant information on the prevailing international and regional standards of protection for particular rights, and also on the approach of other international and regional courts to addressing comparable claims, as well as demonstrating to litigants and others concerned by its rulings that the Court has engaged fully and knowledgably with the relevant arguments'.

[52] Joseph Weiler, 'Editorial: EJIL Vol. 19:5', <http://www.ejiltalk.org/letters-to-the-editor-respond-to-ejil-editorials-vol-195/>, describing the approach of the CJEU in the *Kadi* judgment (Joined Cases C-402 & 415/05P, Kadi & Al Barakaat Int'l Found. v. Council & Commission, [2008] ECR 1-6351).

[53] See letter of 31 July 2014 from Google Global Privacy Counsel Peter Fleischer to Isabelle Falque-Pierrotin, Chair of the Article 29 Working Party, <https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit>, at 11.

earlier. This is consistent with surveys that have shown that 'the majority of European Internet users would want to claim their 'right to be forgotten''.[54] The Article 29 Working Party has embarked on a dialogue with three leading search engine providers (Google, Microsoft, and Yahoo)[55] which is apparently designed to lead to it issuing a set of guidelines on the questions raised by the judgment, and Google has since released a summary giving more information about its approach to dealing with suppression requests.[56] But more information is needed about issues such as what types of Internet services are covered; what information is required from an individual to make a request; what sorts of requests are received; what search domains are covered; and what the procedure is for evaluating a request.

Ideally this information would be compiled by a neutral third party, but it seems that only the search engines themselves have access to detailed information about the requests to exercise the right that are made to them. It is not clear that there is any mechanism for compelling search engines to turn over such data, failing a complaint being made to a DPA or court. However, search engines and DPAs will hopefully agree on a cooperative procedure for compiling and sharing such information, such as currently seems to be underway under the auspices of the Article 29 Working Party and which would be in the interest of all sides.

C. IMPLEMENTATION OF THE RIGHT

The Court put the burden of implementation almost completely on data controllers, with involvement of courts and DPAs only foreseen in response to a complaint concerning a decision by the controller.[57] This approach has been criticized, since it seems to allow Internet companies to decide on the scope of application of the fundamental right to data protection.[58] Expecting data controllers to be the primary decision-makers concerning application of the right is surprising in view of the strong emphasis the CJEU has placed in other cases on the necessity for enforcement of data protection rights by independent data protection authorities.[59] The Court might have referred in some way to the need

---

[54] Special Eurobarometer 359, 'Attitudes on Data Protection and Electronic Identity in the European Union', June 2011, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf>, at 158.

[55] See n 16 above.

[56] See letter of 31 July 2014 from Google Global Privacy Counsel Peter Fleischer (n 53).

[57] See para. 77 of the judgment, stating 'Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.'

[58] See, e.g., Meg Leta Ambrose, 'EU Right to be Forgotten Case: The Honorable Google Handed both Burden and Boon', 19 May 2014, <http://playgiarizing.com/2014/05/19/eu-right-to-be-forgotten-case-the-honorable-google-handed-both-burden-and-boon/>.

[59] See Case C-518/07 Commission v. Germany, 9 March 2010, <http://curia.europa.eu/juris/document/document.jsf?docid=79752&doclang=en>; Case C-614/10,

for dialogue between data controllers and supervisory authorities in setting the parameters for how the right is implemented, or could have tailored the compliance duties it expects search engines to follow more precisely.

The judgment requires not just an application of the fundamental right to data protection, but a balancing between the various right concerned.[60] The Court did not expressly list all the rights at issue, but besides data protection and privacy this must include freedom of expression and information.[61] Private companies are simply not in a position to make complex decisions on the balancing of different fundamental rights, a task that is difficult even for courts, data protection authorities, and academics. It is thus essential that the procedures for deciding on suppression requests involve the data protection authorities to some extent. One way to do this could be to agree on a code of conduct or code of practice involving both private sector data controllers and the supervisory authorities, as foreseen by the proposed EU Data Protection Regulation.[62]

It will also be necessary to find a way to automate decisions about whether or not to suppress a link to search results. The volume of suppression requests is already so large that it seems nearly impossible to decide them quickly if each one is considered individually. For instance, taking just the 91,000 requests for suppression that Google says it received by 18 July 2014, if only 10 minutes were devoted to each case, and assuming a team of 100 persons trained in fundamental right law working 8 hours per day, it would still require almost 190 days, or over half a year, to resolve all of them. Further review of such requests by DPAs and national courts would only lengthen the process, and the number of requests could increase greatly if they start being made in large numbers to web sites other than search engines. As this does not represent a satisfactory remedy for individuals, some automated procedure, perhaps involving a code of conduct or the use of technology, seems necessary to ensure that individuals can assert the right to suppression in an effective manner.[63]

Commission v. Austria, 16 October 2012, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=519542>.

[60] See paras. 74, 76, and 81 of the judgment regarding the necessity of a balancing process.

[61] See Article 11 of the EU Charter of Fundamental Rights.

[62] See Article 38 of the proposed EU General Data Protection Regulation (n 12), referring to the possibility of categories of data controllers and processors to draw up codes of conduct, which they can then submit for approval to the Commission or the DPAs.

[63] See para. 58 of the judgment, mentioning the need to ensure 'the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure', and para. 84, emphasizing the need for 'effective and complete protection of data users'.

V. CONCLUSIONS

The judgment is a harbinger of the future of EU data protection law under the Lisbon framework and the proposed EU General Data Protection Regulation. While the parameters of the 'right to be forgotten' proposed under the Regulation are not identical with the those of the right to suppression affirmed in the judgment,[64] the proposed Regulation addresses the same basic issue considered there, namely the difficulty of limiting access to data once they are made available on the Internet.[65] The judgment gives increased urgency to finalizing and enacting the EU reform proposals, since they provide the EU legislator with the opportunity to refine and further specify the right to suppression beyond what a court can do in a single judgment.

The accomplishment of the judgment is to clarify the application of EU data protection law to the Internet, and to affirm the right to suppression of personal data in the context of Internet search engines. The judgment also demonstrates how enactment of the Lisbon framework strengthens the standards for data protection under EU law, particularly as it was issued barely a month after the CJEU invalidated the EU Data Retention Directive based on fundamental rights considerations in the case *Digital Rights Ireland*.[66] The fact that the Court was unwilling to reach a result that would have effectively exempted search engines from the requirements of EU data protection law is also not unexpected.[67]

However, as the Article 29 Working Party has recognized, 'data protection rules only contribute to the protection of individuals if they are followed in practice'.[68] European human rights law also requires that remedies for data protection violations be effective in practice as well as in law.[69] The major question concerning the judgment is thus whether it will really lead to a greater protection of online data protection rights in practice. The answer to this question is uncertain, so that the judgment is like a medieval cathedral that is only half-finished and may take a great deal longer before its final impact can be evaluated.

---

[64] The differences between Article 17 of the proposed EU General Data Protection Regulation (n 12), which deals with the so-called right to be forgotten, and the CJEU's holding are too complex to go into here. See also the Advocate General's opinion (n 13), para. 110.

[65] See, e.g., Recital 53 of the proposed EU General Data Protection Regulation (n 12), stating in part 'This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet'; Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age', 22 January 2012, <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm>, stating 'The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public. The right to be forgotten will build on already existing rules to better cope with privacy risks online'.

[66] C-293/12 and C-594/12, 8 April 2014.

[67] See in this regard Hielke Hijmans, 'Case C-131/12, Google Spain and Google Inc v. AEPD et Costeja Gonzalez', *Maastricht Journal of European and Comparative Law* (forthcoming, 2014).

[68] Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP 12, 24 July 1998), at 5.

[69] See, e.g., Rotaru v Romania (2000) ECHR 191, at para. 67.

Of course, the Court's main task was to answer the questions referred to it. But it could have provided more detail concerning key points such as the types of Internet services the judgment applies to; whether it is limited to searches based on a person's name; the domains that are covered; and the territorial application of the judgment. Given the implications of expecting private sector data controllers to resolve complex balancing situations involving fundamental rights, it could also have been expected that the Court would send a signal that cooperation with the DPAs is essential in this regard. However, the Court failed to explore in sufficient detail some issues that were important to provide full answers to the questions referred to it, such as application of the balancing test involved in applying the right to suppression.[70] The judgment's minimalist style fails to fully address the relevant issues and the global impact of the case, and can only diminish the respect given to the judgment outside the EU.

A fuller discussion of the judgment's implications for the Internet would also have strengthened the Court's reasoning. For example, it may be asked how the Court can conclude that the rights of data subjects protected by Articles 7 and 8 of the Charter (i.e., the rights to privacy and data protection) override as a general rule the interest of Internet users (para. 81) when it never explains what that interest is. This willingness to give data protection interests priority over other fundamental rights is a leap of logic requiring fuller explanation than the Court gave, as does its assumption that the risks presented by the Internet are greater than the benefits it brings.

While the Court's inclination to provide strong protection to online data protection rights is laudable, the judgment is thus less impressive in its consideration of the case's long-term implications. This indicates that the Court has not yet found a way of applying the Lisbon framework to online data processing in a way that provides effective protection in practice as well as in theory. The judgment provides a strong affirmation of online data protection rights, but fails to indicate a way forward for their effective implementation and realization, the development of which will likely be a struggle for data controllers, DPAs, and courts.

The protection of individual rights in practice has traditionally been one of the main weaknesses of EU data protection law,[71] and at the moment there is no reason to believe that the situation will be different with regard to the right to suppression. One can also ask why so much public attention is being given to the 'right to be forgotten', while other important data protection issues languish in relative obscurity.[72]

---

[70] See on this point Steve Peers, 'The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression', 13 May 2014, <http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html>.

[71] See, e.g., European Commission, 'First Report on the Implementation of the Data Protection Directive (95/46/EC)', 15 May 2003, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=en>, at 12.

[72] For example, the fact that many DPAs in the EU apparently lack the financial and human resources to carry out their functions receives little media attention. European Union Agency for Fundamental Rights,

The questions raised in this article concerning the scope of the judgment can undermine the intellectual coherence of the right to suppression if they are not adequately addressed. If the material and territorial scope of the right are disproportionately broad, DPAs will not be able to oversee its implementation in a way that protects fundamental rights, given the limited resources they have at their disposal and the fact that their enforcement jurisdiction ends at the borders of their respective Member States.[73] The wording of the judgment does not exclude a wide interpretation of the judgment's scope, but this will likely have to be specified by further court decisions and DPA action as the judgment is implemented. A way must be found to make the scope of the right to suppression proportionate to the ability to implement it in practice, if it is not to become so all-encompassing as to be meaningless.

Finding that the fundamental right of data protection applies to Internet search engines should be the beginning, not the end, of the discussion.[74] We must move beyond the affirmation of data protection rights under the Lisbon Treaty to find a way to implement them that leads to effective protection in practice. This will be a work in progress, as data controllers struggle to develop a procedure for balancing different rights, DPAs find a role in overseeing implementation, and courts deal with disputes concerning the right to suppression that are brought before them. Hopefully a code of conduct or some other cooperative mechanism that is applicable on an EU-wide basis can be developed in this regard. The decisive question is whether data controllers and the DPAs will be able to implement the judgment effectively and in a way that respects both data protection and other fundamental rights.

'Data Protection in the European Union: the Role of National Data Protection Authorities' (2010), <http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf>, at 42.

[73] Regarding the territorial jurisdiction of the DPAs, see EU Data Protection Directive, Article 28. See also Digital Rights Ireland, C-293/12 and C-594/12, 8 April 2014, para. 68, stating that it cannot be fully assured that data stored outside the EU are subject to control by the EU DPAs.

[74] See James Griffin, *On Human Rights* (OUP 2009), at 95, stating that a '[h]uman right can be at stake in ways that are not especially important […]'