Google v. Spain:
A Right To Be Forgotten?

Ignacio Cofone*

Abstract

The comment shows that the recent decision in Google v. Spain *does not rule on the right to be forgotten, but rather on the liability of search engines under the rights and obligations established in the Data Protection Directive. It then makes a brief evaluation on the case arguing that the decision fails to offer a consistent balance between the right to privacy and the freedom of expression.*

Introduction

The right to be forgotten was popularized in the public debate by Mayer-Schönberger's book *Delete*.[1] The book argued that one of the main problems with data storage is that it lacks the human characteristic of forgetting.[2] The book also introduced "the right to forget", proposing that all information should have an expiration date.[3] Policymakers, especially in the European Union (EU), were sympathetic to the concept.[4]

The right to be forgotten extends to the internet the old French *droit à l'oubli* and the Italian *diritto al' oblio* regarding criminal records—sometimes called right to oblivion, and literally translatable as right to forget. Both rights were affirmed by courts based on the constitutional dispositions stating that prison has the aim of social reinsertion, and it is in the interest of both social reinsertion and the privacy of people who were

---

* Erasmus University Rotterdam (European Doctorate in Law and Economics). I am grateful to Tobias Hlobil, Stephan Michel, Sharon Oded, Pablo del Rio and Ann-Sophie Vandenberghe for helpful comments and discussions. The standard disclaimer applies. Contact: cofone@law.eur.nl. Burgemeester Oudlaan 50, 3062PA Rotterdam, The Netherlands.

[1] Some precedents can be seen before that in reviews of European legal thought regarding privacy. *See e.g.* David H. Flaherty, *Controlling Surveillance: Can Privacy Protection be Made Effective?*, in TECHNOLOGY & PRIVACY: THE NEW LANDSCAPE 167, 172 (Philip E. Agre and Marc Rotenberg eds., Cambridge, MIT press, 1998); Jean-François Blanchette & Deborah G. Johnsson, *Data Retention and the Panoptic Society: the Social Benefits of Forgetfulness*, 18(1) THE INFORMATION SOCIETY 33 (2002).

[2] *See* Viktor Mayer-Schönberger, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 92-127 (2009).

[3] *See id.* at 169-195.

[4] *See* Jeffrey Rosen, *The Right to be Forgotten*, 64 STANFORD LAW REVIEW ONLINE 88, 89 (2012).

convicted for the records to be erased after some time. For data protection, European policymakers decided to take the matter one step further.[5]

In the next section, the right to be forgotten is briefly explained. Section three summarizes the case of Google v. Spain, and section four evaluates the rights provided by the Data Protection Directive invoked in that case. Section five explains the difference between the right to be forgotten and the rights provided under the Data Protection Directive, and section six offers a criticism of the ruling. Finally, section seven concludes.

I. The Right to be Forgotten

The right to be forgotten has been a concrete topic of debate in EU policy, its importance increasing since Commissioner Reding presented the General Data Protection Regulation proposal in 2012.[6] The regulation—proposed to be operative in the EU in 2015—follows the general principles of the Data Protection Directive[7] while also incorporating additional elements including the right to be forgotten.

In an illustrative classification, Fleisher offers three interpretations of the right to be forgotten.[8] First, and least controversially, the right to be forgotten can mean that one has the right to delete the information one posts online. Many—although not all—social network sites already allow for this. Secondly, it can mean that one has the right to delete any information about oneself that one posts online, including information that others have re-posted. Third, it can mean that one has the right to eliminate any information that is available online about oneself, regardless of origin.

As the General Data Protection Regulation proposal stipulates, the right to be forgotten allows data subjects to request a data controller, at any time, to remove from their database any piece of information regarding that data subject, regardless of the source of the information.[9]

---

[5] While the right to forget focuses on the expiration of information after some time, the right to be forgotten focuses on the control over one's personal information. *See* Rolf H. Weber, *The Right to Be Forgotten More Than a Pandora's Box?*, 2 JIPITEC 120 (2011).

[6] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter, Regulation Proposal].

[7] Directive 1995/46/EC.

[8] *See* Peter Fleischer:Privacy…?, *Foggy Thinking About the Right to Oblivion*, (Mar. 9, 2011), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

[9] *See* Vivianne Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INTERNATIONAL DATA PRIVACY LAW 3 (2011).

Article 17(1)[10] outlines four possible conditions for this right to be claimable.

The first condition requires that the data is no longer necessary for the purpose for which it was collected (purpose limitation principle).[11] The second condition occurs when the data subject revokes consent when such consent was required for the collection of the data.[12] The third condition requires that the data subject exercise the right to object.[13] The fourth condition occurs when the collection or processing of the data violates any provision of the regulation.[14]

The second condition incorporates a new element of the right to be forgotten in the European data protection system: revocation of consent of the data subject *without the need to prove harm*. The other three are already present, albeit less systematically so, in the Data Protection Directive.[15]

This second condition refers to Article 6(1), which defines the legitimate collection and processing of personal data, particularly as it pertains to consent. This proposal means that data subjects can request the elimination of their personal data from a database in situations where the subject's consent was originally the basis for acquiring or otherwise processing the data, based solely on a change of mind without needing to prove to a court that the subject suffered actual harm.[16]

II. Google v. Spain

Shortly after the second anniversary of the regulation proposal, the European Court of Justice (ECJ) ruled on *Google v. Spain*. In 2010, Mario Costeja requested that Google and the Spanish newspaper La Vanguardia remove two articles published January 19, 1998 and March 9, 1998 (along with the corresponding links in the search engine), which reported details of a government auction on his house due to his failure to pay social security debts.[17]

---

[10] *See also* Regulation Proposal, *supra* note 6, Recitals 53 - 54.
[11] *See id.* at art. 17(1)(a); *see generally infra* note 41 and accompanying text.
[12] *See id.* at art. 17(1)(b).
[13] *See id.* at art. 17(1)(c).
[14] *See id.* at art. 17(1)(d).
[15] *See* Meg Leta Ambrose & Jef Ausloos, *The Right to be Forgotten Across the Pond*, 3 JOURNAL OF INFORMATION POLICY 1, 12 (2013).
[16] If the data was acquired based on legitimizing reasons other than consent then Article 17(1)(b) is not applicable. This limitation is relevant since parts (b) to (f) of Article 6(1) contain legitimating purposes that could be applicable; concretely, the existence of a contract (Article 6(1)(b)), of a legal obligation (Article 6(1)(c)), vital interest of the data subject (Article 6(1)(d)), public interest (Article 6(1)(e)), and legitimate interests of the data controller (Article 6(1)(f)). Directive 1995/46/EC.
[17] *See Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014 E.C.J. C-131/12, ¶ 14 (May 13) [hereinafter, Google].

The Spanish Data Protection Authority did not back the claim against the newspaper due to the fact that the information was published lawfully. However, it did order Google Spain SL and Google Inc. to "take steps to remove its index data and preclude future access to the same". Both Google Spain SL and Google Inc. appealed the resolution, and the case arrived to the court Audiencia Nacional.[18]

Audiencia Nacional requested a preliminary ruling from the ECJ.[19] In the request, the court was asked three questions: (i) if the European data protection framework established in the Data Protection Directive is applicable to Google, (ii) if search engines are considered data controllers under the Directive, and (iii) if a data subject can demand a search engine to remove the indexation of a certain piece of information.[20]

Regarding the first question, the advocate general and the court agree that the European framework does apply to Google, not because it is dealing with EU citizens, but because Google Spain is a subsidiary of Google Inc. situated in Spanish territory which sells advertisement spots in Spain that, in turn, finance the search engine. Therefore, even if data is not processed in Spain, the processing is done within the context of the activities of an establishment in a member state of the EU.[21] This part of the ruling confirms a previously issued opinion by Article 29 Working Party, which has expressed an equivalent position for the applicable law of the directive.[22]

Regarding the second question, both the advocate general and the court noted that Google is dealing with personal information. The court further affirmed that by indexing data, Google retrieves, records and organizes data, even if Google's indexing is done automatically without distinguishing content and when this data was previously published elsewhere. Accordingly, the Court treats Google (and other search engines) as a controller, with the duties that such classification implies under the Directive.[23]

The third question is the most relevant for the purposes of this comment. The question reads:

> *"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*

[18] *See id.* at ¶¶ 15-18.
[19] *See generally* Consolidated Version of the Treaty on the Functioning of the European Union art. 267, 2008 O.J. C 115/47 [hereinafter TFEU].
[20] *See Google*, 2014 E.C.R. C-131/12 at ¶¶ 19-20.
[21] See id.
[22] *See* Working Party on the Protection of Individuals with regards to the Processing of Personal Data, "Opinion 8/2010 on Applicable Law," Dec. 16, 2010.
[23] *See Google*, 2014 E.C.R. C-131/12 at ¶¶ 66-88.

> *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?'"* [24]

Regarding this question, the court considered that, if the inclusion of certain links in the search results is at some point in time incompatible with the provisions of the Directive, and the data subject requests so, such links must be erased. The Court emphasized that, due to Article 7 of the Directive, data processing must be lawful at all times in order to be allowed to be continued.[25] In addition, even information initially collected in a lawful way can - with the passing of time - become unlawful to maintain when the data becomes inadequate, irrelevant, or excessive for the purposes of the processing.[26]

For data processing to be incompatible with the Directive, the data does not necessarily have to be incorrect. It is sufficient that the data is inadequate or excessive for the purpose of the data processing, that it is outdated or that it is kept for a time longer than necessary for such purpose.[27] The court noted that sensitive information contained in sixteen year old search links, can fall under the aforementioned categories.[28]

As a response to the ruling, Google established a governance mechanism on May 30th through which European data subjects can now fill an online form to request that obsolete data about them be deleted from the lists of results.[29] The search engine has already received more than 70,000 requests.[30]

III. Applicable Norms

The court explains that the preliminary ruling is centrally concerned with Articles 2(b), 2(d), 4(1)(a), 4(1)(c), 12(b) and 14(1)(a) of

---

[24] *Id.*
[25] *See id.* at ¶ 95.
[26] See id.
[27] *See Google*, 2014 E.C.R. C-131/12 at ¶¶ 72, 92-9; Directive 1995/46/EC at art. 6(c)-6(e).
[28] *See id* at ¶¶ 94-98.
[29] Online form at https://support.google.com/legal/contact/lr_eudpa?product=websearch
[30] *See* Rosa Jimenez Cano, *Google comienza a aplicar el 'derecho al olvido'*, EL PAIS, (Jul. 13, 2014), http://tecnologia.elpais.com/tecnologia/2014/07/03/actualidad/1404405567_813834.html.

Directive 95/64/EC.[31] While Article 2 concerns definitions and Article 4 concerns applicable national law, Article 12 refers to the right to erasure and Article 14 to the right to object.[32] The latter two articles are relevant for the third question posed.[33]

The directive contains a similar right to the one proposed in Article 17 of the regulation proposal in Article 12(b) and Article 6(1)(e). However, only the second condition of that article is new.[34] Article 12(b) of the directive establishes the right to erasure, which allows data subjects to request the elimination of their personal data when its retention or processing violates the terms of the directive, in particular (but not exclusively) because of being incomplete or inaccurate.

While a narrow reading of the article will interpret "in particular" as "exclusively" and will only allow the deletion of the data when such data is incomplete or inaccurate, a broad reading will allow for such deletion whenever the data processing is in violation of any term of the directive.[35]

In turn, the directive establishes the purpose-limitation principle in Article 6(1)(e);[36] accordingly any collection, processing or storing of personal data must be done based on a specific, explicit and legitimate purpose.[37] The last of the three requirements indicates that companies need a legitimizing basis to collect personal data, of which the most common is consent.[38]

Data cannot be kept for longer than is necessary for the purposes for which it is collected or processed—a purpose that is defined, however, by the data controller. This rule is extended to secondary use, according to which the data is retained for a legitimate purpose that is different than its original purpose.[39] This obligation for data controllers and data processers can be invoked, if original purpose terms are violated, by data subjects

---

[31] *See Google*, 2014 E.C.R. C-131/12 at ¶ 1.
[32] The court also mentions later on Articles 6, 7, 9 and 28. *See id.* at ¶ 1.
[33] *See id.* at ¶ 89.
[34] *See* Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows. A Critical Analysis of "The Right to be Forgotten" in Big Data Practice*, 8(3) SCRIPTED, 230, 232-233 & 240-245 (2011).
[35] This, as it was seen, is similar to the fourth element of Article 17 of the regulation proposal. *See* Regulation Proposal, *supra* note 6.
[36] *See generally* Working Party on the Protection of Individuals with regards to the Processing of Personal Data, 2013 O.J. 03/2013.
[37] The Directive is applicable, according to its Article 2(a), whenever there is collection, processing or storing of personal information, where personal information is defined as any information that can be traced back to a data subject. Directive 1995/46/EC.
[38] Consent is defined in Article 2(h) of the Data Protection Directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement". Directive 1995/46/EC.
[39] *See* Bert-Jaap Koops, *The Inflexibility of Techno-regulation and the Case of Purpose-binding*, 5 LEGISPRUDENCE 171 (2011).

claiming the right to erasure contained in Article 12(b) when interpreted broadly,[40] as Costeja seems to have done.

The right to object is recognized in Article 14 of the Directive. It establishes that a data subject, proving compelling legitimate grounds relating to a particular situation, can object to the continued processing of his personal data. If a data subject does object, and he can successfully prove compelling legitimate grounds, then the controller must stop processing the data subject's personal data, although is the controller has no duty to eliminate data already processed.[41]

IV. Different Rights

Under the classification made above on the possible interpretations of the right to be forgotten, the regulation proposal would establish the third, most expansive category of the right, while the data protection directive does not establish any of the three classifications. Under the third category, the right to be forgotten would likely involve not only the publisher of the content but also search engines that link to that content.[42] This, however, does not mean that any involvement of search engines in terms of liability for published content pertains the right to be forgotten.

As can be seen in the previous sections, none of the three questions presented to the court are, strictly speaking, about the right to be forgotten. Even though the third question is related to it, and although Audiencia Nacional asked it mentioning the right to be forgotten,[43] the actual question refers in its formulation only to the rights of erasure and the right to object.[44]

The opinion of the advocate general, in turn, is clear in stating that the rights to erasure (Article 12(b)) and the right to object (Article 14(a)) in the Data Protection Directive are not equivalent to the right to be forgotten. The opinion is categorical in pointing out that the right to be forgotten is nowhere to be found in the current EU legal framework for cases in which the publication of information is de facto legitimate. European data protection law does not provide a right to eliminate truthful but embarrassing information.[45]

---

[40] *See Koops*, *supra* note 34 at 10.

[41] Individuals have a right to withdraw their consent when they desire to, but this withdrawal only affects future processing. This means that data subjects do not have, under the current directive, the right to request the elimination of any data solely based on the withdrawal of consent. *See* Working Party on the Protection of Individuals with regards to the Processing of Personal Data, 2008 O.J. 15/2011.

[42] *See Rosen*, *supra* note 4.

[43] Concretely, "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")". *Google*, 2014 E.C.R. C-131/12 at ¶ 20.

[44] *See Google*, 2014 E.C.R. C-131/12 at ¶¶ 66-88.

[45] *See Google*, 2014 E.C.R. C-131/12 at ¶ 17.

Even when deciding differently than the advocate general, the ECJ seems to maintain this principle in its ruling. The court extends the broad reading of Articles 12 and 14 of the directive to hold that any information that is no longer relevant violates the directive, and its elimination can be therefore requested by invoking the right to erasure.

The central difference between the right to erasure and the right to be forgotten is that the latter also includes data that does not breach any norm.[46] This difference might not always be as clear as it seems. A certain processing of information could be considered as breaching a general provision of the directive because it harms a data subject; or, as the court does, because it is no longer relevant, even without being outdated or inaccurate. At the margin, the difference means that with a right to be forgotten, a data subject could request the deletion of the data based on a whim, or a preference, while under the current system there are significant probative and argumentative efforts necessary to prove to a court that such data is harmful and it violates personality rights.[47]

If the right to be forgotten was enforced in the EU data protection system, a data subject's personal information would have to be deleted at his request irrespective of harm or of the legality of the processing—with differing levels of amplitude depending on which of the three versions of the right is enforced. The right, additionally, would likely cover not only links displayed by search engines but also the original publications of the content.

In the form established by Google, however, data subjects' requests must be justifiable and will be evaluated individually on their merit. In that evaluation, the company has the ability to reject them, and those who disagree with the decision made by the company will have to ask a court to intervene. In this way, the result of the case illustrates the differentiating elements between the right to be forgotten and the rights data subjects have under the directive, which someone must evaluate— in this case, Google supervised by the court. Unless European data subjects can prove a violation of the directive and the presence of harm, they will at least for now have to face being remembered.

V. Critical Discussion

Under the E-commerce Directive, internet service providers in the EU are not liable for hosting illegal content; only the users who upload the content are liable.[48] The reason behind this rule is that, otherwise, providers might find themselves forced to police the internet in order to

[46] *See Koops*, *supra* note 34.
[47] *See id.*
[48] Directive 2000/31/EC.

remove content for which they could be held liable.[49] The social costs of such policing activity (both in the form of the actual costs for the company and the costs of the chilling effects it would intake) are likely to be higher than its benefit.[50] The only way to eliminate false negatives would be to incur in false positives, leading to collateral censorship.[51]

Until recently, there was a debate on whether a similar immunity would apply to the data protection directive, both for internet providers and for search engines.[52] *Google v. Spain*, as it was seen, makes it clear that for the moment it will not.

A problem with adopting this decision is that search engines such as Google work with automatic algorithms, which makes it difficult for them to become a censor of what is published and what is not published. Google localizes information but it does not control it; Google cannot make any choices regarding its means and purposes in terms of Article 4(d) of the directive.

This, as the advocate general makes clear in his opinion, makes it close to impossible for Google to make sure all information it indexes complies with Articles 6, 7 and 8 of the directive on data quality. It would be one thing to shift the responsibility from the content creator (in this case, La Vanguardia) to the content indexer (in this case, Google) if (and only if) the content indexer displayed reasonable means to prevent the indexation of such content, but to place search engines as censors of the internet is something else entirely.

Still, this is not the main problem with the *Google v. Spain* decision. The main problem is that free speech is not about being able to express oneself in a vacuum, but about being able to transmit a message to people who want to hear it.

The court argues in the case that the information indexed by Google is not relevant. But the decision begs the question of who decides what is relevant. If what information is relevant enough to be accessed is to be decided neither by people looking for such information nor by the person publishing that information, but centrally decided by a court, both

---

[49] *See* Giovanni Sartor & M. Viola de Azevedo Cunha, *The Italian Google-case: Privacy, Freedom of Speech and Responsibility of Providers for User-generated Contents*, INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 1 (2010).

[50] *See generally* Doug Lichtman & Eric A. Posner, *Holding Internet Service Providers Accountable*, 14 SUPREME COURT ECONOMIC REVIEW 221 (2006); Mark A. Lemley, *Rationalising Internet Safe Harbors*, 6 JOURNAL OF TELECOMMUNICATION AND HIGH TECHNOLOGY LAW 101 (2007); Keith N. Hylton, *Property Rules, Liability Rules and Immunity: An Application to Cyberspace*, 87 BOSTON UNIVERSITY LAW REVIEW 1 (2007); James Grimmelmann, *The Google Dilemma*, NEW YORK SCHOOL LAW REVIEW 939 (2009).

[51] *See* Jack M. Balkin, *The Future of Digital Expression in a Digital Age*, 36 PEPPERDINE LAW REVIEW 101 (2009).

[52] *See* Giovanni Sartor, *Providers' Liabilities in the new EU Data Protection Regulation: A Threat to Internet Freedoms?*, 3(1) INTERNATIONAL DATA PRIVACY LAW 3 3 (2013).

freedom of expression and the right to access information will suffer a blow.

Search engines are not megaphones, sending content unilaterally to passive recipients. Search engines are an intermediary. Recipients of the information which they index choose the results they look for and they choose which web pages from those results they read.

The job of search tools such as Google is to help those internet users find the content they want to find.[53] This means that if a certain piece of information (such as the auction of Costeja's house) appears in the top search results, it does so because a large number of internet users considered it to be relevant: they searched for it, and when coming across the result they opened it.

If there was a problem with search engines leading internet users to find unwanted content by accident, and such content was harmful for other internet users, then search engines would have incentives to correct this as fast as possible.[54] But this is not the problem the court is concerned with.

The court is concerned with people who look for such information and find it, and cobbles a solution allowing for the existence of the information but making it unavailable for the public who look for it on search engines. It is difficult to say, then, that the information is not relevant, and it is hardly consistent to say that the information should be kept online (since it was published legally) but made inaccessible at the same time.[55]

Conclusion

The right to be forgotten can mean different things in the European data protection regime, and *Google v. Spain* seems to pertain to none. With the right to erasure, the right to forget and the right to be forgotten competing as the one to remain as the safeguard of data subjects in European law, confusion is to be expected.

The case is centrally about defining the legal obligations of intermediaries such as search engines under the directive. In it, the ECJ dictates that the processing of data that is no longer relevant violates the terms of the directive and extends the right to erasure and the right to objection to include search engines as a consequence of considering them

---

[53] *See* James Grimmelmann, *Don't Censor Search*, 117 YALE L. J. POCKET PART 48 (2007) (further arguing that his enhances autonomy since locating information is important for making choices, and it is economically efficient by allowing numerous welfare enhancing information exchanges that would otherwise not take place).

[54] See *id.*

[55] See *id.* (stating: "if the content really is sufficiently harmful that its suppression is justified, it would be better to target the owner of the site where it appears. She will typically have better information about what the content is, whether it is false, and who is responsible for creating it").

data controllers (question 2) who fall under the jurisdiction of the European data protection system (question 1).

Defenders of freedom of expression might be relieved. One should not forget, still, how dangerous it can be to censor search.