Orla Lynskey

Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez

Article (Accepted version) (Refereed)

Original citation:
Lynskey, Orla (2015) *Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez.* Modern Law Review, 78 (3). pp. 522-534. ISSN 0026-7961

DOI: 10.1111/1468-2230.12126

Abstract: In the Google Spain judgment, the Grand Chamber of the EU's Court of Justice determined the circumstances in which a search engine is obliged to remove links to data pertaining to an individual from the results displayed by its search engine. The Court also considered the material and territorial scope of the EU data protection rules. This note argues that the Court's findings, which have been heavily criticised, are normatively coherent. The broad scope of application of data protection rules and the right of individuals to have their data deleted when certain conditions are fulfilled both play a part in granting individuals effective control over their personal data - an objective of EU data protection law.

Keywords: data protection, privacy, EU charter, search engine, freedom of expression, intermediary liability

Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costjea Gonzalez*

Orla Lynskey*

INTRODUCTION

After almost two decades of obscurity, data protection law has been propelled intothe limelight in recent years. The reform of the EU data protection regime proposed by the European Commission in 2012, the Snowden revelations of 2013 and the first use of the EU Charter to annul an entire piece of secondary legislation – the Data Retention Directive – have all contributed to the rise to prominence of this longstanding policy. The most recent data protection development to attract widespread global attention has been the judgment of the Court of Justice (the Court) in *Google Spain*[1], discussed in this note.

In *Google Spain* the Court was asked to determine what obligations – if any – EU data protection law imposes on search engines, in this instance Google, vis-à-vis individuals who seek to suppress information relating to them which is lawfully available online. The Court held that when a person is searched for by name in Google's search engine, Google is obliged to remove links to web pages from the results its search engine displays if the processing of this data is incompatiblewith the provisions of the Data Protection Directive. These links must be removed irrespective of whether the web pages themselves continue to be lawful. It has been this finding of the Court which provoked the most controversy, in particular because of the Court's failure to address its freedom of expression implications. At the heart of the matter is the divisive issue of default control over information: should individuals be entitled to control the dissemination of their personal data or should the claim that this information belongs in the public domain prevail?

FACTUAL BACKGROUND

*Assistant Professor of Law, London School of Economics and Political Science.

[1] Case 131/12, *Google Spain SL, Google Inc*. v *Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECR I-000, nyr.

Mr Costeja Gonzalez was involved in insolvency proceedings relating to social security debts in the late 1990s. These proceedings were reported in a regional newspaper in Spain in 1998 and the article was later made available online. Mr Costeja Gonzalez, who was named in the report, asked the newspaper to delete the piece arguing that the insolvency proceedings were concluded and it was no longer of relevance. The newspaper refused to erase the data on the basis that the Ministry of Labour and Social Affairs had ordered its publication. Mr Costeja Gonzalez also asked Google Spain to remove links to the newspaper in its search results when his name was entered as a search term in the Google search engine: Google Spain sent this request to Google Inc. in the United States.

Mr Costeja Gonzalez theno addressed a complaint to the Spanish Data Protection Authority (DPA). The DPA rejected the complaint against the newspaper on the grounds that the publication of such data in the press was legally justified. However, the DPA upheld the complaint against Google Spain and Google Inc., requesting that the contested links be removed from Google's index of search results.

Google sought the annulment of this decision before the *Audencia Nacional* which stayed the proceedings in order to refer a number of questions to the Court of Justice. The questions referred to the Court can be grouped into three sets of issues relating to, first, the material scope of application of the Data Protection Directive; second, its territorial scope of application; and third, the application of the data subject's right to delete personal data under existing data protection rules. Advocate General Jääskinen was tasked with delivering an Opinion on the proceedings. The Court and the Advocate General agreed on the Directive's territorial scope of application. However, this was one of the rare instances in which the Court departed from the Advocate General's Opinion: its findings differed significantly from those of the Advocate General on the material scope of the Directive and, ostensibly, on the substantive issue concerning the data subject's right to delete. More fundamentally, as will be discussed below, the Court's judgment and the Advocate General's Opinion reveal their differing conceptions of the desired role of data protection in the EU legal order.

THE MATERIAL AND PERSONAL SCOPE OF THE DIRECTIVE

In order to determine whether the Data Protection Directive[2] applied to Google's search engine activities, the Spanish court asked the Court of Justice whether the activities of a search engine constitute 'processing of personal data' for the purposes of Article 2(b) of the Directive and, if so, whether a search engine operator is a 'data controller' within the meaning of Article 2(d).

Article 2(b) of the Directive defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'. It then goes on to give a non-exhaustive list of such operations. The Court noted that the activities of a search engine – which 'collects', 'retrieves', 'records', 'organises', 'discloses'

[2] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/23.

and 'makes available' personal data – must be classified as 'processing'.[3] Google had argued that knowledge of the data – in particular, whether specific data are personal or not – was required for operations to be classified as 'processing'[4], an argument which was rejected by the Court.[5] Neither, according to the Court, did Google need to alter the data already published online for its actions to constitute data processing[6] as to require such alteration would be to deprive the Directive of its effect.[7]

The Court then considered whether Google constituted a 'data controller'. A 'data controller' is an entity which 'alone or jointly with others determines the purposes and means of the processing of personal data'.[8] Obligations are place on data controllers pursuant to the Directive. In opining that Google was not a 'data controller', the Advocate General emphasised that Google does not distinguish between source web pages which contain personal data and those which do not.[9] In particular, he specified that the files which Google processes contain 'personal data and other data in a haphazard, indiscriminate and random manner'.[10] He proposed a factual rather than a formalistic assessment of whether an entity is responsible for data processing and suggested that such responsibility should hinge on whether the entity responsible was firstly, 'aware of the existence of a certain defined category of information amounting to "personal data"' and, secondly, that the controller 'processes this data with some intention which relates to their processing as personal data.'[11]

The Court, however, refused to encompass a 'knowledge' or 'intention' criterion in the notion of 'data controller'. Resorting to both a literal and teleological interpretation of the Directive, the Court held that a search engine should not be excluded from the definition of controller[12] and,in this way, the Court preserved the broad personal scope of application of the Data Protection Directive.

THE TERRITORIAL SCOPE OF THE DATA PROTECTION DIRECTIVE

Article 4(1) of the Directive determines its territorial scope of application. It provides that the rules of a Member State apply when, inter alia, the processing is carried out by a data controller established in a Member State or if a controller established outside the EU makes use of equipment on the territory of the Member State for the purposes of processing.

Google argued that it was neither established nor making use of equipment in Spain and therefore did not fall within the scope of Spanish data protection rules in this context. It argued that Google Spain acts only as a commercial representative of Google for its advertising activities – promoting and selling advertising space on Google – and is not

[3] n 1 above at [28].
[4] *ibid* at [22].
[5] *ibid* at [28].
[6] *ibid* at [29]
[7] *ibid* at [30].
[8] n 2 above Article 2(d).
[9] n 1 above at [72].
[10] Opinion of Advocate General Jääskinen in Case 131/12, *Google Spain SL, Google Inc*. v *Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECR I-000, nyr at [81].
[11] *ibid* at [82].
[12] *ibid* at [34].

involved in the search engine activities under examination. Moreover, it denied that it 'makes use of equipment' for the provision of search engine services in Spain claiming that the use of web spiders to index content does not constitute 'use of equipment'.

The Advocate General and the Court of Justice were in agreement that Google Spain did fall within the territorial scope of the Directive with both taking a functional approach to Article 4(1). The Advocate General emphasised the need to take the business model of internet search engines into consideration. The provision of free search engine services is cross-subsidised by the revenue generated by keyword advertising services. Therefore, a company is established in a Member State for the purposes of the Directive if the revenue-generating limb of the enterprise, which subsidises the technical processing operations taking place elsewhere, is established in that Member State.[13] The Advocate General opined that Google should be viewed as a single economic unit, a concept borrowed from Competition law, for the purposes of establishing the territorial applicability of the Directive.[14]

The Court reached an identical conclusion by aligning itself more closely to the Directive's wording. It noted that, pursuant to the Directive's recitals, 'establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements'.[15] As Google Spain engages in such effective and real exercise of activity through stable arrangements, it constitutes an establishment.[16] The question was then whether the relevant personal data processing was 'carried out in the context of the activities' of its establishment. The Court distinguished between processing carried out 'by' the established entity and processing carried out 'in the context of the activities' of the establishment.[17] It found that the processing of personal data for Google's search engine services was processing 'carried out in the context of the activities' of Google Spain's establishment as Google Spain promoted and sold advertising space in Spain which rendered Google's search engine services profitable.[18] This cross-subsidisation 'inextricably links'[19] the activities of the search engine and its establishment in Spain: a finding to the contrary would compromise the effectiveness of the Directive according to the Court.[20] This finding is in keeping with the Court's insistence that a broad interpretation of the Directive's territorial scope was intended by the legislature and necessary in order to ensure the effective and complete protection of fundamental rights.[21]

THE RIGHTS FLOWING FROM THE DATA PROTECTION DIRECTIVE

Perhaps the most contentious issue before the Court was whether an obligation flowed from the provisions of the Directive – in particular Articles 12(b) and 14(a)– for a search engine operator to remove links to (otherwise) lawful material published on third party webpages.

---

[13] *ibid* at [67].
[14] *ibid* at [66].
[15] n 1 above at [48].
[16] *ibid* at [49].
[17] *ibid* at [52]
[18] *ibid* at [55].
[19] *ibid* at [56].
[20] *ibid* at [58].
[21] *ibid* at [53] and [54].

It follows from Article 12(b) of the Directive that data subjects have the right to obtain from the data controller 'the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data'. The Court noted that the examples of incompatible data processing in Article 12(b) are not exhaustive.[22] It recalled that in order to be compatible with the Directive processing must also comply with the data quality principles in Article 6 and have a legitimate legal basis pursuant to Article 7.[23] The legal basis for data processing in the present case was Article 7(f)[24] which permits data processing that is necessary for legitimate interests pursued by the controller or third parties to whom the data are disclosed, except where these interests are overridden by the rights and freedoms of the individual data subject. It therefore requires a balancing of 'the opposing rights and interests of the data subject and the data controller, while taking into account the Charter rights to data protection and privacy.'[25] The reliance on Article 7(f) as a legal basis for the data processing brings Article 14(a) into the legal picture. This provisionallows the data subject to object to processing conducted on the basis of Article 7(f) by advancing compelling legitimate grounds relating to his particular situation, save where otherwise provided by national legislation.[26]

The Court identified the data subject's right to privacy and data protection on the one hand and the 'interest of internet users in having access to information' on the other as the opposing interests in this case. It noted that while 'as a general rule' the data subject's right to privacy and data protection override the interest of internet users in having access to information, the balance in specific cases may depend on other factors, such as the nature of the data and whether the public had an interest in it.[27] It therefore held that, if necessary to comply with Articles 12(b) and 14(a), a search engine operator must remove links to web pages which are indexed when a person is searched for by name even if those web pages are themselves lawful.

The Court advanced several factors to support this finding. Most significantly, it stated that a search engine operator does not appear to benefit from the derogation to the Directive for processing carried out 'solely for journalistic purposes'.[28] It also stated that the balancing exercises conducted under Articles 7(f) and 14(a) differ depending on whether the processing is conducted by a publisher or a search engine operator because processing by a search engine is likely to constitute a more significant interference with the right to privacy than publication on a web page.[29]

Having determined the extent of the responsibility of a search engine operator pursuant to these provisions, the Court considered the scope of the rights granted to data subjects. In particular, it considered whether the removal of links could be justified on the basis that the

[22] *ibid* at [70].
[23] *ibid* at [71].
[24] *ibid* at [73].
[25] *ibid* at [74].
[26] *ibid* at [76].
[27] *ibid* at [81].
[28] *ibid* at [85].
[29] *ibid* at [86] and [87].

information they contained may be prejudicial to the data subject or that he simply wished it to be forgotten. The Court reiterated that when a data subject makes a request pursuant to Article 12(b), the compatibility of the processing with the Directive is dependent upon compliance with the Article 6 safeguards (therefore processing must not be irrelevant, excessive, outdated etc).[30] Equally, if Article 7(f) is relied upon to legitimise data processing, the processing must be authorised on this basis for the entire period during which it is carried out.[31] The Court therefore emphasised that when appraising requests opposing data processing, the individual's right is not contingent on this indexed information causing prejudice to him or her.[32] The Court concluded that the fundamental rights to privacy and data protection should, 'as a rule' override both the economic interest of the search engine operator as well as the interest of the general public in finding the information.[33] However, in certain circumstances, there may be a preponderant interest of the general public (for instance, if the individual concerned was a public figure).[34] The Court advised the Spanish referring Court, who would ultimately decide on this matter, that no such preponderant interest appeared to exist in the case before it, highlighting the sensitivity of the information in question for the data subject's private life and that its initial publication had taken place 16 years previously.[35]

The Court's judgment has significant normative and practical implications, all of which it is impossible to catalogue. This comment shall focus on the following: the continued use of the misleading 'right to be forgotten' label in the wake of the judgment, the judgment's implications for the development of the Charter's right to data protection and its relevance to 'Cyber-lawyers'.

THE MISLEADING 'RIGHT TO BE FORGOTTEN' LABEL

In finding that a search engine's obligation to remove links relating to an individual from its index is not contingent on that indexed information causing prejudice to the individual, the Court was not finding that a 'right to be forgotten' exists. Rather, it follows from the Court's judgment that such prejudice is neither necessary nor sufficient: the right to delete only applies when the data processing is incompatible with the Directive. To label such a right a 'right to be forgotten' is misleading.

Moreover, while the findings of the Court appeared, at first sight, to depart from those of the Advocate General on this matter, both in fact agreed that an individual has no general right to prevent the indexing by internet search engines of potentially prejudicial personal information available on third party web pages. The Advocate General's examination was limited to the question of whether 'a subjective preference alone'[36] amounts to a compelling legitimate ground within the meaning of Article 14(a) and therefore whether the processing

[30] *ibid* at [92].
[31] *ibid* at [95].
[32] *ibid* at [96].
[33] *ibid* at [97].
[34] *ibid* at [97].
[35] *ibid* at [98].
[36] n 10 above at [108].

was compatible with the Directive. On this narrow question of whether 'subjective preference alone' should be decisive, the Court agreed with him that it should not.

This critical distinction between, on the one hand, the right to erasure if processing is incompatible with the provisions of the Directive and, on the other, a right to be forgotten based on an individual's personal preferences has not been adequately recognised and has enabled the judgment's implications to be exaggerated. For instance, in its report on the subject, the House of Lords EU Committee misinterprets the European Commission's intervention in the proceedings. The Commission had argued that the Article 12(b) right to delete applies where processing does not comply with the Directive 'from which it follows that this right does not confer on the data subject an absolute right…simply because he believes that this may be prejudicial to him, or because he wishes the information to be consigned to oblivion'.[37] The Commission was clearly here highlighting the distinction made above and not, as the Committee report suggests, arguing against the Court's ultimate finding. This misleading 'right to be forgotten' label should therefore be abandoned.

MAKING AN ENTRANCE: THE RIGHT TO DATA PROTECTION

The EU Charter of Fundamental Rights provides for a right to data protection alongside, but independently of, the established right to privacy. The relationship between these two rights is contested, with some arguing that data protection is merely a subset of the right to privacy while others advocate that it is an independent right. For instance, in the UK data protection has traditionally been treated as a facet of privacy[38] although the distinction between the two rights was highlighted by a High Court judge in 2013 in order to limit the justiciability of the Charter right to data protection in the UK.[39] The EU Courts have consistently conflated the rights to data protection and privacy, thereby further muddying the waters. While in this case the Court continued to refer to the rights to data protection and privacy in the singular, its judgment provides an indication of the additional role it foresees for the right to data protection in the EU legal order.

The judgment provides implicit support for the recognition of 'control over personal data', irrespective of whether these personal data are 'private', as a fundamental aspect of the right to data protection. Data protection experts have long-suggested that this control, sometimes referred to in stronger terms as 'informational self-determination', is a central aspect of data protection. Indeed, the idea of 'informational self-determination' is one which was recognised by the German Constitutional Court in 1983 in its Population Census decision'[40] when the Court found that individuals must, in principle, have the capacity to determine whether their data are disclosed and the use to which they are put. Nevertheless, there are no references to this 'informational self-determination' or even the notion of 'control' in the wording of the Charter right to data protection or in the Data Protection Directive. 'Enhanced individual control' has however featured prominently in the discourse regarding the data

[37] Quoted at [47] in HL 40 (2014).
[38] See, for instance, *Durant* v *Financial Services Authority* [2003] EWCA Civ 1746, Auld LJ at [28].
[39] *R (on the application of AB)* v *Secretary of State for the Home Department* [2013] QB 3453 at [16].
[40] Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65, 1.

protection reform package currently making its way (slowly) through the European legislative process. Recital 6 of the Proposed Regulation states that 'Individuals should have control over their own personal data' and reflects the Commission's stated aim to 'put individuals in control of their own data'.[41] An additional recital suggested by the European Parliament rapporteur which stated that the right to the protection of personal data is based on the right of the data subject to exert control over the personal data that are being processed' would have made this control dimension even more explicit however it was removed from the final text agreed upon by Parliament.[42]

In addition to this elucidation of the normative underpinning of the right to data protection, the judgment also seeks to enhance the practical effectiveness of this right.[43] The Court's refusal to incorporate the subjective element of 'awareness' into the notion of 'data controller' as suggested by the Advocate General is just one such example. The Court instead preferred to adopt a literal interpretation of this concept in order to preserve the Directive's broad scope of application, emphasising the importance of this broad scope for the effectiveness of data protection rules.[44] Perhaps more critically, in finding that Google may be under an obligation to remove links, the Court held that the effective and complete protection of individuals could not be achieved if these individuals were required to also have this information erased from the initial host publisher.[45]

The Court's implicit endorsement of individual control over personal data and its explicit emphasis on the effectiveness of the right to data protection have been welcomed by data protection and privacy advocates. However, as is often the case when the law seeks to regulate technology, it may be too late. In an era of Big Data and ambient technologies it is arguably naïve to believe that individuals can exercise effective control over their personal data. Constructs which are central to the effectiveness of data protection law are challenged by these societal developments: for instance, the principle of 'purpose limitation' pursuant to which data should be collected for 'specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes'[46] directly contradicts the logic of Big Data, which is to mine huge volumes of data (including personal data) to discover correlations. In this case, the Advocate General encouraged the Court to reject what he termed a 'maximalist approach' to data protection rules[47], as it had done in *Lindqvist*[48], highlighting that the Directive had been drafted in a pre-Internet era.[49] Likewise, scholars

[41] 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 (General Data Protection Regulation), COM (2012) 11 final, 2.
[42] European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)).
[43] See, n 1 above at [30], [34], [38], [53], [58] and [84].
[44] *Ibid* at [34].
[45] *ibid* at [84].
[46] n 2 above Article 6(1)(b).
[47] n 10 above at [79].
[48] Case 101/01 *Bodil Lindqvist* [2003] ECR I- 12971.
[49] n 10 above at [77].

such as Koops have argued that data protection law is based on a number of fallacies, including that it can be effective and can promote individual control over personal data. Koops argues that in order to survive data protection must begin to look in other regulatory directions.[50] While this may be true, it is not reflected in the current data protection reform package which further complicates the data protection law thicket and does little to clarify how data protection should be reconciled with competing interests, such as innovation.

The Court's alleged failure to reconcile the right to data protection with the competing rights to receive and impart information has also been criticised. While the Court acknowledged the 'decisive role' played by search engines in disseminating data[51], its failure to refer directly to the right to freedom of expression enshrined in Article 10 ECHR and Article 11 EU Charter is remarkable. The Court stresses the privacy and data protection implications of search engine operators' ability to aggregate information, create personal profiles and to widely and easily disseminate these aggregated profiles.[52] However, it does not acknowledge that the removal of data from a search engine rather than a web page also has more significant freedom of expression implications for the very same reasons: it prevents easy access to data for a larger number of individuals. While not explicitly stated, the Court appears to assume that when the rights to privacy and data protection are at stake the right to freedom of expression extends only to 'public interest' information – as opposed to information in which the public may have an interest. Again, it is suggested that this finding is entirely consistent with data protection's role of enhancing individual control over personal data. Nevertheless, it puts the EU on a collision course with the United States where the First Amendment right to freedom of speech is treated as an 'argumentative showstopper'. Perhaps ironically given the firm rejection of European-style rights balancing in First Amendment jurisprudence and scholarship, the judgment has attracted a lot of criticism in the United States for its failure to grant adequate weight to the right to freedom of expression. The judgment is possibly best viewed as an attempt by the Court of Justice to establishes data protection as Europe's 'argumentative showstopper' in the wake of international data protection and privacy scandals.

A TEXTBOOK CASE-STUDY FOR CYBER-REGULATION?

The judgment also provides plenty of food for thought for those working in the field of Internet law and may even provide a further basis to respond to Easterbrook's scathing critique of Cyberlaw: that it is as useful as the Law of the Horse. Several of the challenges regulators and search engines are grappling with in the aftermath of this judgment – online jurisdiction, decentred regulation and the responsibilities of internet intermediaries – are familiar issues to Cyberlawyers.

The Court's functional approach to the territorial scope of the Data Protection Directive enabled the Spanish DPA to assume jurisdiction in the present case. This approach may be

[50] B. Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250, 261.
[51] n 1 above at [36]
[52] *Ibid* at [38] and [87].

relatively uncontroversial when the data controller is based within the EU and hence EU data protection rules de facto apply. However, the judgment raises two more controversial jurisdiction issues. First, the judgment enables the EU to claim jurisdiction over processing which occurs outside the EU borders when the data controller has a relevant revenue-generating subsidiary in the EU even if the decisions regarding data processing are taken beyond EU borders. Secondly, it begs the question of whether the judgment requires Google to modify its search results globally or to attempt to identify Google users within the EU through territorial domain name extensions or geographic filtering tools. Imposing an obligation on Google to modify its Google.com search results may appear like a disproportionate expansion of the EU's jurisdiction given the accuracy of filtering techniques yet such an approach has been supported by the EU's influential Article 29 Working Party.[53] Such territorial differentiation is not new[54] but does further balkanise the internet which is arguably becoming increasingly less global in nature.

In practice, the Court's judgment also imposes an obligation on Google to determine whether particular personal data is in the 'public interest', a task traditionally vested in trusted public authorities rather than private enterprises governed by commercial imperatives. Such 'decentred' regulation is commonplace online but poses particular challenges. In this instance, it allows a private entity to define the contours of a public debate: Google has done this by, first, framing the question for consideration and, second, influencing the forum for debate.Google has set about examining 'How should one person's right to be forgotten be balanced with the public's right to information?'.[55] This framing of the question is problematic. First, it refers to a 'right to be forgotten' which, as discussed above, is misleading. Secondly, it pits data protection as an individual right against freedom of expression as a societal right. However, data protection and privacy, like freedom of expression, serve societal objectives by preventing the chilling of individual behaviour. Moreover, Google has influenced the forum for debate by establishing an 'Advisory Council' which held a European road show canvassing opinion in order to 'help it navigate the issue'. This proactive attempt to engage with interested members of the public has been criticised as Google has 'handpicked the members of the council, will control who is in the audience, and what comes out of the meetings'.[56] Finally, the judgment raises queries regarding Google's status as an internet intermediary in the context of its provision of search engine services and whether, as such, it should benefit from intermediary liability exemption. Indeed, the Advocate General opined that the Google search engine is a passive intermediary which has 'no relationship with the content of the third-party source web pages which it copies'.[57] In

[53] Article 29 Working Party, 'Guidelines on the Implementation fo the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12', delivered on 26 November 2014 (WP225/14).
[54] *Licra et UEJF* v *Yahoo! Inc. and Yahoo! France* T.G.I. Paris, 22 May, 2000.
[55] Google Advisory Council website at https://www.google.com/advisorycouncil/ (last accessed 13 January 2016).
[56] This is the opinion the President of the EU's Article 29 Working Party, an advisory group on data protection matters, expressed to Reuters. 'Google hosts meetings across Europe on privacy rights' 8 September 2014, http://www.reuters.com/article/2014/09/08/us-google-privacy-idUSKBN0H308I20140908 (accessed 14 November 2014).
[57] n 10 above at [86].

reaching this conclusion, the Advocate General pointed to recital 47 of the Data Protection Directive as well as Articles 12 to 14 of the E-Commerce Directive[58] which suggest that facilitating the technical transmission of content does not create control over this content.[59] Further support for the proposition that Google's search engine services benefit from such intermediary liability could be garnered from the Opinion of Advocate General Maduro in *Google v Louis Vuitton* which was not referred to in the present case.[60] Advocate General Maduro suggested that the aim of the intermediary liability provisions was to create a 'free and open public domain on the interent' by limiting the liability of neutral intermediaries.[61] He provided Google's search engine as an example of such a neutral service to which the provisions ought to apply.[62] However, whether search engine services do, and should, benefit from the intermediary liability shield provided for by the E-Commerce Directive is contested. Article 21 states that in examining the need for an adaptation of the Directive, a European Commission report shall 'analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services'. This suggests that the Directive does not yet address the issue of search engine liability for third party content.[63] Furthermore, whether search engine activites should benefit from such an exemption is also questionable given that search engines offer no warranties in terms of objectiveness, completeness or neutrality.

However, irrespective of whether the provsions of the E-Commerce Directive apply to search engines, Google would not be exempt from its responsibilities under data protection law in this instance. Pursuant to Article 1(5)(b) of the E-Commerce Directive, it does not apply to 'questions relating to information society services' covered by the Data Protection Directive.[64] That Google is not in this instance a beneficiary of an exemption for internet intermediary liability is therefore not as incongruous a finding as one may initially assume.

CONCLUSION

Depending on one's point of view, the judgment's implicit emphasis on individual control over personal data and explicit emphasis on the effectiveness of the right to data protection may be seen as either the first step in the resurrection of a floundering data protection regime or its last gasp. The judgment is certainly divisive. In the hearing before the House of Lords EU Select Committee, invited witnesses disagreed on whether Google should be viewed as a data controller and on the feasibility of implementing the judgment. The Committee's report, concluded that a 'right to be forgotten…is as elusive as its name is misleading'.[65]

---

[58] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.
[59] *ibid* at [87].
[60] Opinion of Advocate General Jääskinen in Joined Cases C-236/08 – 238/08, *Google France* v *Louis Vuitton* [2010] ECR I–2417.
[61] *ibid* at [142].
[62] *ibid* at [144].
[63] B van Alsenoy, A Kuczerawy and J Ausloos et al, 'Search Engines after Google Spain: Internet@Liberty or Privacy@Peril', 63. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494## (last accessed 14 November 2014).
[64] Article 1(5)b of the E-Commerce Directive.
[65] HL 40 (2014), 21.

Despite this damning assessment of the judgment and its implications, it is uncertain what impact it will have on the ongoing data protection reform process. What was once termed 'a right to be forgotten' has been renamed 'a right to erasure' in the current draft text. The European Parliament seeks to extend this right to erasure in certain circumstances to apply not only vis-à-vis data controllers but also third parties which have linked to or copied the data in question.[66] While this extension is likely to be contested in Council on feasibility grounds, the judgment is likely to bolster the resolve of those involved in the European legislative process to forge on with the reform package. Whether this package succeeds in delivering effective control over personal data, only time will tell; for now, all that happens must *not* be known.[67]

[66] European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), Article 17.

[67] D. Eggers, *The Circle* (San Francisco: McSweeney's, 2013). Eggers' fictional tale seeks to illustrate how privacy is socially constructed and deconstructed. It depicts the life of an employee of a social media company whose objective is total transparency from cradle to grave and whose company credo is 'All that happens must be known'.