Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González: An Entitlement to Erasure and Its Endless Effects

I. OVERVIEW

In the modern age, you can bet that any potential employer has Googled your name prior to your interview and already knows your 2008 Halloween costume, your boyfriend's middle name, and that your name is written on the ceiling at Lucy's Bar. But fear not, millennials, times are changing! No longer will you have to deactivate your Facebook whilst job searching or hear parental lectures about how they "never did that in college," knowing fully well that they did—photographic proof just does not exist. In a recent decision, the Court of Justice of the European Union (CJEU) issued an opinion that places a new obstacle in the way of those trying find out personal information about others via the Internet, impeding access to information that used to be just a click away.[1]

The court's recent decision provides individuals with the right to require a search engine operator to remove search result links that appear when specific key terms are Google searched if those links contain certain personal information.[2] In its 2014 decision, the court ordered Google Inc. and its subsidiary, Google Spain, to remove two links that appeared when Mario Costeja González's name was typed into the Google Spain search engine bar.[3] The links led to two newspaper articles published by the *La Vanguardia* in 1998 concerning a real estate auction connected with proceedings for the recovery of social security debts.[4] González filed his original complaint with the Agencia Española de Protección de Datos (Spanish Data Protection Agency) (AEPD), alleging

1. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX 62012CJ0131, ¶ 99 (May 13, 2014).
2. *Id.*
3. *Id.* order 3.
4. *Id.* ¶ 14.

that the information was irrelevant because the related matters had since been resolved.[5] He claimed that the Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 (Directive) ensured his right to privacy and that the laws of the Directive allowed him to request the removal of links within the search results.[6] González requested that the newspaper be required either to remove the articles so the identifiable personal data no longer existed or to protect the data by use of search engine tools.[7] Additionally, he requested that Google Spain and Google Inc. be required to remove or hide his personal data so that it no longer appeared in the list of links that resulted from a search of his name.[8] The AEPD rejected the complaint against La Vanguardia because the information had been lawfully published, but partially ruled in González's favor and ordered the removal of the links from Google's search producing page.[9] Google Spain and Google Inc. appealed the decision, and the case was brought before the Audiencia Nacional (National High Court).[10] The court chose to stay the proceedings and referred their questions about the Directive to the CJEU for a preliminary ruling.[11] The CJEU *held* that in order to comply with the Directive, Google Spain and Google Inc. must remove the links at González's request in order to respect his right to privacy. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 EUR-Lex CELEX 62012CJ0131 para. 99 (May 13, 2014).

II. BACKGROUND

The rationale behind the creation of the Directive was to "protect[] the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[12] Though technological data-processing systems in today's world operate to assist people, the Directive was created to ensure that the rights of those people, specifically the rights of freedom of expression and to privacy, remained protected and intact.[13] Since its creation, multiple courts have referred questions concerning the Directive to the CJEU for

5. *Id.* ¶¶ 14-15.
6. *Id.* ¶ 23.
7. *Id.* ¶ 15.
8. *Id.*
9. *Id.* ¶¶ 16-17.
10. *Id.* ¶ 18.
11. *Id.* ¶ 20.
12. *Id.* ¶ 3.
13. *Id.*

clarification and preliminary rulings.[14] Specifically, the court has been asked to interpret the scope of the Directive, to whom and to what it applies, and most relevantly, in what circumstances does the right to request removal apply.[15]

However, personal data can be processed as long as it falls under one of the several exceptions provided for in the articles of the Directive.[16] Specifically, the exceptions within article 7 state that personal data can be processed only if the data subject has given his or her consent, the processing of the data is necessary for compliance with a legal obligation, or the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority that is vested in the controller or a third party to whom the data are disclosed.[17] Additionally, article 13 of the Directive allows Member States to derogate from the Directive's provisions if its purpose is to "safeguard a number of objectives in the public interest," in particular if those interests are of economic or financial importance.[18]

In the court's analysis of the interference caused by the data processing, a balancing test is applied where the data processor's right to freedom of expression must be weighed against the seriousness of the interference with the privacy rights of the data subject.[19] The Directive further requires that the interference be lawful and necessary for the pursuit of legitimate aims.[20] Furthermore, article 9 of the Directive reconciles the pull between the fundamental rights of the controller and those of the data subject by permitting the processing of personal data when it is "carried out solely for journalistic purposes or the purpose of artistic or literary expression," equalizing the processor's and the data subject's rights.[21]

---

14. *Id.* ¶ 20; Joined Cases C-465/00, 138/01 & 139/01, Rechnungshof v. Österreichischer Rundfunk, 2003 E.C.R. I-4989, ¶ 23; Joined Cases C-92/09 & 93/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, ¶ 35; Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy (*Satamedia*), 2008 E.C.R. I-9831, ¶ 34; Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12971, ¶ 18.

15. Case C-131/12, *Google Spain*, ¶ 20; Joined Cases C-465/00, 138/01 & 139/01, *Österreichischer*, ¶ 23; Joined Cases C-92/09 & 93/09, *Volker*, ¶ 35; Case C-73/07, *Satamedia*, ¶ 34; Case C-101/01, *Lindqvist*, ¶ 18.

16. *See* Joined Cases C-92/09 & 93/09, *Volker*, ¶ 7; Case C-73/07, *Satamedia*, ¶ 7.

17. Joined Cases C-92/09 & 93/09, *Volker*, ¶ 5.

18. Joined Cases C-465/00, 138-01 & 139-01, *Österreichischer*, ¶ 58.

19. *Id.* ¶ 84.

20. *Id.* ¶ 51.

21. Case C-73/07, *Satamedia*, ¶ 7.

In the past, courts have referred their questions to the CJEU, asking for the interpretation of the terms and phrases used in the Directive.[22] Though it is the not the job of the court to resolve factual disputes, the court has the responsibility to interpret European Union (EU) law and settle legal disputes between EU governments and EU institutions.[23] Additionally, the court ensures that the laws of the EU are uniformly applied.[24] The court has previously issued opinions in which it interpreted the fundamental phrase used in the Directive, "the processing of personal data."[25] Article 2 of the Directive defines the term personal data as "any information relating to an identified or identifiable natural person," while processing is defined as "'any operation or set of operations which is performed upon personal data, whether or not by automatic means' . . . including disclosure by transmission, dissemination or otherwise making data available."[26] The court has suggested that the Directive's use of broad terms is intended to prevent the restriction of its application.[27]

The court's decision in *Criminal Proceedings Against Bodil Lindqvist* demonstrated just how comprehensive the court believes the Directive's language should be.[28] The court applied the Directive to a modern-day issue and held that the act of placing information on an Internet site falls within the Directive's definition of "processing" because it entails the loading of a page onto a server, a partly automatic operation.[29] When that information contains identifiable personal information, it constitutes a processing of personal data.[30] Years later, the court expanded this application and held that even the elongated process

---

22. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX 62012CJ0131, ¶ 20 (May 13, 2014) (discussing a request from the Audiencia Nacional of Spain for an interpretation of the meaning of the word "establishment" and the phrase "use of equipment . . . situated on the territory of the said Member State" in the context of the Directive); Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12971, ¶ 18 (asking if the actions of the defendant constituted a "processing of personal data"); Case C-73/07, *Satamedia*, ¶ 34 (asking if the sharing of data relating to earned and unearned income and assets of people via text message constituted a "processing of personal data").

23. *Court of Justice of the European Union*, EUR. UNION, http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm (last visited Mar. 15, 2015).

24. *Id.*

25. Case C-101/01, *Lindqvist*, ¶¶ 24-27.

26. *Id.* ¶¶ 24-25.

27. *See* Joined Cases C-465/00, 138/01 & 139/01, Rechnungshof v. Österreichischer Rundfunk, 2003 E.C.R. I-4989, ¶ 73; Joined Cases C-92/09 & 93/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, ¶¶ 51, 59.

28. Case C-101/01, *Lindqvist*, ¶¶ 95-99.

29. *Id.* ¶ 26.

30. *Id.* ¶ 27.

of collecting documents, transferring them onto a CD-ROM, and then processing them so they could be transmitted via text message to subscribers comprised the processing of data.[31]

Additionally, the court has addressed the issues that follow when personal data that has previously been published in the media is further processed and made available to third parties.[32] In *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy*, the court held that even personal information that had previously been published could be "processed" in terms of the Directive when it was republished in its unaltered form.[33] The court reasoned that because none of the exculpating exceptions applied, the scope of the Directive must be interpreted to encompass the publishing of this kind of information.[34] The court went on to interpret article 9 of the Directive, examining the meaning of the phrase "solely journalistic purposes."[35] The court looked at the reconciliation phrasing provided by article 9 and decided that, to avoid the obstruction of freedom of expression, the few exceptions apply only when strictly necessary.[36] The journalistic activities that the exceptions cover only include those where the objective is to disclose information, opinions, or ideas to the public, regardless of the medium used to communicate the information.[37]

The balance between the rights of controllers and data subjects is one that courts have been continuously asked to weigh and evaluate.[38] In *Rechnungshof v. Österreichischer*, the court was asked to determine if certain objectives claimed by the Rechnungshof (Court of Audit) outweighed the privacy rights of the defendant data subjects whose names and financial information were published and made available to the general public.[39] The Rechnungshof argued that the publication of a report that listed the names, yearly salaries, and pensions of those whose earnings exceeded a certain amount was exempt from the Directive under article 13 and was thus lawfully published.[40] It claimed that though the publication could be considered an interference with the data subjects'

---

31. Case C-73/07, *Satamedia*, 2008 E.C.R. I-9831 ¶ 37.
32. *Id.* ¶¶ 35-63.
33. *Id.* ¶ 49.
34. *Id.* ¶¶ 39-46.
35. *Id.* ¶ 50.
36. *Id.* ¶ 56.
37. *Id.* ¶ 61.
38. *See* Joined Cases C-465/00, 138/01 & 139/01, Rechnungshof v. Österreichischer 2003 E.C.R. I-4989, ¶ 84; Joined Cases C-92/09 & 93/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, ¶ 77.
39. Joined Cases C-465/00, 138/01 & 139/01, *Österreichischer*, ¶ 23.
40. *Id.* ¶ 58.

private lives, the interference was justified because the publication was in the pursuit of a legitimate objective: to ensure transparency in order to keep salaries at a low level so that public funds are used economically and efficiently.[41]

In its opinion, the court quoted language from article 6 of the Directive and explained that data "must be 'collected for specified, explicit and legitimate purposes' . . . and must be 'adequate, relevant and not excessive' in relation to those purposes."[42] The court analyzed the interference caused by the publication of the personal data and found that although the mere collection of the monetary information was not interference, the communication of it to third parties, by means of the report, was.[43] The court added that regardless of the subsequent use of the data, it still has the ability to interfere with the private lives of data subjects.[44] Additionally, the court noted that both the character of the interference and whether it had inconvenienced the data subjects were irrelevant.[45]

However, the court acknowledged that the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) was additionally applicable in this case.[46] Under article 8 of the ECHR, when the processing is lawful, pursues one or more of the specified legitimate aims, and is necessary in a democratic society in order to achieve those aims, it is permissible, regardless of the Directive.[47] The court found that the interference of the Rechnungshof was in accordance with the law and that it pursued the legitimate aim to promote the economic well-being of the state, therefore meeting two of the three qualifications of the ECHR.[48] In conclusion, the court left the actual balancing up to the national court. If the national court determined that the publication of the data was necessary for and appropriate to the objectives claimed by the Rechnungshof, then the processing was permissible.[49]

Years later, the court was again asked to conduct a balance-of-interests test.[50] The court acknowledged the existence of the right to

41. *Id.* ¶¶ 5, 50.
42. *Id.* ¶ 66.
43. *Id.* ¶ 74.
44. *Id.*
45. *Id.* ¶ 75.
46. *Id.* ¶¶ 10, 71.
47. *Id.* ¶ 76.
48. *Id.* ¶¶ 77, 81.
49. *Id.* ¶¶ 88-90.
50. Joined Cases C-92/09 & 93/09, Volker und Markus Schecke GbR v. Land Hessen 2010 E.C.R. I-11063, ¶ 77.

privacy and the protection of data, but stated that those rights were not absolute and were only to be considered in the formulation of its decision.[51] The court was asked to weigh what was claimed to be a legitimate interest against the rights of data subjects when a searchable website made personal information about beneficiaries available to the general public.[52] In its opinion, the court insinuated that the principle of transparency can act as a legitimate, justifiable interest because the publishing of certain information by a government entity enables the public to participate more directly in the decision-making process and ensures accountability in a democratic system.[53] However, an interest in transparency has no priority over the right to the protection of personal data.[54] The interest must still be balanced against the interference conferred on the rights of those whose personal data is being publicized.[55]

In the case at hand, the court explained that it did not appear as though the Council of the European Union and the European Commission that had published the personal data took other methods into consideration before broadcasting the information to the general public.[56] It seemed that other methods could have been employed that would have caused less interference with the beneficiaries' private lives.[57] For instance, the court suggested that the published information could have been limited to the names of the individuals, rather than coupling their names with the amount of money they had received.[58] The court determined that a balance between the rights of the publishers and of the data subjects could have been reconciled by other means that were not examined or employed.[59] Therefore, the publication exceeded the limits of the Directive and had to be removed from the website.[60]

III. THE COURT'S DECISION

In the noted case, the CJEU was again asked to interpret the Directive in order to reach a decision in a case.[61] The court addressed the novel issues that arose after a search engine provided links as results if

51. *Id.* ¶¶ 47-48.
52. *Id.* ¶ 35.
53. *Id.* ¶¶ 68-71.
54. *Id.* ¶ 85.
55. *Id.* ¶ 77.
56. *Id.* ¶ 81.
57. *Id.* ¶¶ 81-83.
58. *Id.* ¶ 81.
59. *Id.* ¶¶ 81, 86.
60. *Id.* ¶ 86.
61. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX 62012CJ0131, ¶ 20.

they led to websites containing personal data.[62] To reach its decision, the court examined the territorial scope of the Directive, the Directive's provisions as they applied to search engines, and a data subject's right to require search engines to remove links from their search results if they led to websites containing their personal information.[63] The court held that because of the subsidiary nature of Google Spain (under the authority of Google Inc.) and the activities it completed within the Member State, both companies were subject to the laws of the Directive.[64] Additionally, the court held that the broad language of the Directive should be interpreted to mean that a search engine operator can be regarded as a "controller" of data processing and that the activities of collecting, indexing, and providing information in the form of search results was within the Directive's definition of a "processing of personal data."[65] The court determined that to comply with the Directive, a search engine operator is obligated to remove the links that lead to the data subject's personal information if that information has certain qualifications.[66] With this decision, the court created a "right to be forgotten."[67]

At the start of its opinion, the court reiterated the objective the Directive aims to accomplish: the protection of fundamental rights and freedoms, specifically the right to privacy with respect to the processing of personal data.[68] The court quoted the Directive, emphasizing language that implies an extended scope covering all instances of personal data processing regardless of whether that processing is done by a person in a different country.[69] The court then addressed article 6, in which the Directive lists what constitutes lawful data processing.[70] The article requires Member States to process personal data "fairly and lawfully [and] collect[] [it only] for specified, explicit and legitimate purposes."[71] Additionally, the data must be relevant, accurate, kept up to date, and not excessive in relation to the purposes for which it is collected.[72] As in its preceding decisions, the court in the noted case acknowledged that the Directive provides exceptions, such as those contained in article 7, that

62. *Id.*
63. *Id.* ¶¶ 21-99.
64. *Id.* ¶ 60.
65. *Id.* ¶ 41.
66. *Id.* ¶¶ 88, 98.
67. *Id.* ¶¶ 20, 91.
68. *Id.* ¶ 3.
69. *Id.*
70. *Id.* ¶ 7.
71. *Id.*
72. *Id.*

address journalistic works and data processing done in furtherance of a legitimate interest.[73]

In the substance of its opinion, the court addressed three particular questions asked by the referring court.[74] The first asked whether the actions of Google Spain, a subsidiary of Google Inc., were subject to the provisions of the Directive when Google Inc., the parent company, is located in the United States, outside of the Member State of Spain.[75] Google Spain is a version of Google Search offered in Spanish.[76] It is operated by its parent company, Google Inc., which is located in the United States.[77] Google Search sends out crawlers or robots that "locate and sweep up the content of web pages methodically and automatically" and then index that information for people to search.[78] Although Google Search does not provide direct access to the information on the indexed websites, it provides a list of relevant search results and profits on advertisements that correspond with the Internet users' search terms.[79] Google Spain acts as a commercial agent and controller for Google Search and promotes the sale of advertising space in Spain.[80] Specifically, Google Spain's objectives are to "promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising."[81]

Article 4 of the Directive declares that the legislation applies both when the processing of the data is carried out "in the context of the activities of an establishment of the controller on the territory of the Member State" and when the controller is not established in the Member State, but uses equipment within the Member State to process data.[82] The referring court asked for interpretations of the word "establishment" and the phrase "use of equipment situated on the territory of the said Member State."[83] Evidently, it was unclear if the language should be read to mean that the Directive applied to the situation in the noted case.[84]

As it had done so in the past, the court explained that the wording of the Directive must not be interpreted restrictively because its objective is

---

73. *Id.* ¶¶ 8-9.
74. *Id.* ¶ 20.
75. *Id.*
76. *Id.* ¶ 43.
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.* ¶ 6.
83. *Id.* ¶ 44.
84. *Id.*

to ensure the utmost protection for data subjects.[85] The court concluded that because Google Spain is a subsidiary of Google Inc. and engages in activity within Spain, it must be considered as an "establishment" for the purposes of the Directive.[86] Although the actual processing of the data is performed by Google Inc. and Google Spain merely provides support by promoting the sale of advertising space, the court explained that article 4 of the Directive does not require the processing of personal data to be carried out exclusively by the establishment; it only requires that the processing be carried out in context of the activities of the establishment.[87] Additionally, the court added that the legal form of the establishment, subsidiary, or parent, is not a dispositive factor in the analysis of the Directive's application.[88] Therefore, the court decided that it must follow that the processing performed by Google Spain fits the Directive's meaning of being "carried out 'in the context of the activities' of that establishment."[89] The court held that because of the "inextricable link" between the actions carried out by Google Spain for the purposes of serving Google Inc., it must be concluded that both fall under the territorial scope of the Directive.[90] Thus, the court concluded that when the operator of a search engine establishes a subsidiary in a Member State and the job of that subsidiary is to promote and sell advertising space, the Directive has controlling authority.[91]

The second question the court was asked to answer inquired whether the actions of Google Search qualified as a processing of personal data within the meaning of the Directive and, if so, who the acting controller was.[92] Google Spain and Google Inc. argued that because the company merely provides Internet users with a list of search results, it does not process personal data.[93] The court returned to the language used in the Directive and explained that the "processing of personal data" included activities "such as the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure [of information] by transmission, dissemination or otherwise."[94] It is the job of a search engine operator to collect data from

85. *Id.* ¶¶ 53-54.
86. *Id.* ¶ 49.
87. *Id.* ¶ 52.
88. *Id.* ¶ 48.
89. *Id.* ¶ 55.
90. *Id.* ¶¶ 47, 60.
91. *Id.* ¶ 60.
92. *Id.* ¶ 20.
93. *Id.* ¶ 22.
94. *Id.* ¶ 25.

third-party websites, record and organize that data, and then index and store it on servers before making it available to users in the form of a list of search results.[95] Therefore, the court found that it must conclude that the activities of Google Spain and Google Inc. were included within the Directive's definition of "processing."[96]

Furthermore, the court found it necessary to clarify that even though the case concerned only the display of links that led to websites containing personal data, the action completed in order to display those links constituted a processing of personal data.[97] As it had established in prior decisions, the court explained that just because the data had already been published on the Internet by a third party and remained unaltered by the search engine, the search engine's operators were not exempt from the Directive's provisions.[98] The court cited its prior decision in *Satamedia* and explained that giving immunity to this kind of action would counteract the underlying objectives of the Directive.[99]

The court then turned its attention to the second portion of the question that concerned the meaning of the word "controller."[100] The Directive defines "controller" as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[101] Again, the court emphasized that the language of the Directive must be interpreted loosely in order to accomplish broad application and appropriate protection for all data subjects.[102] The court reasoned that because a search engine operator determines the purposes and means that are employed to complete the data processing, they are therefore within the definition provided by the Directive.[103] The court explained that a search engine operator further acts as a controller because as a search engine indexes the data it collects, it makes it easier for Internet users to find specific information on particular individuals.[104] This facilitation heightens the likelihood that the privacy rights of an individual will be

95. *Id.* ¶ 28.
96. *Id.*
97. *Id.* ¶ 57.
98. *Id.* ¶¶ 29-30; *see also* Case C-73/07, *Satamedia*, 2008 E.C.R. I-9831, ¶¶ 48-49.
99. Case C-131/12, *Google Spain*, ¶ 30.
100. *Id.* ¶ 32.
101. *Id.*
102. *Id.* ¶ 34.
103. *Id.* ¶ 33.
104. *Id.* ¶¶ 37-38.

significantly affected and infringed upon.[105] Therefore, Google Spain and Google Inc. qualify as controllers under the Directive.[106]

The last question the court was asked to answer related to a data subject's potential "right to be forgotten."[107] The referring court asked if articles 12 and 14 of the Directive should be interpreted to mean that a data subject has the right to require the operator of the search engine to remove certain links from a list of search results on the grounds that the information might be prejudicial to him or her.[108] Article 12 allows for the erasure or blocking of data that does not comply with the provisions of the Directive because of its "incomplete or inaccurate nature."[109] This includes data that is irrelevant, not kept up to date, or kept longer than necessary.[110] The court explained that under this provision, the Directive affords data subjects the right to demand the removal of their personal data if, over the course of time, it has become incompatible with the Directive.[111] Regardless of whether the information is true or if it is lawfully published, if it is determined that the processed data does not conform to the provisions of the Directive, the provided link must be removed from the list of search results.[112]

However, the court still had to weigh the interests of Google Spain and Google Inc. against González's.[113] The court determined that the sensitivity of the published information and the fact that the topic had since become irrelevant due to the passage of time and the settlement of the issue merited a right to request the removal of the links from the search results.[114] Although the economic interests of Google Inc. and Google Spain paired with the general public's interest in finding out general information were relevant, the court determined that González's right to privacy outweighed those rights.[115] Therefore, the court held that González had a right to the removal of the particular links from the list of search results and that the operators must comply with his request.[116]

---

105. *Id.*
106. *Id.* ¶ 41.
107. *Id.* ¶ 20.
108. *Id.* ¶¶ 20, 89.
109. *Id.* ¶ 10.
110. *Id.* ¶ 92.
111. *Id.* ¶¶ 92-93.
112. *Id.* ¶ 94.
113. *Id.* ¶¶ 96-98.
114. *Id.* ¶ 98.
115. *Id.* ¶¶ 97-98.
116. *Id.* ¶ 99.

IV. ANALYSIS

The concept of privacy falls on a sliding scale. At one end, people believe that it is a right that should be afforded to all and are willing to go to great lengths to ensure that right. On the opposite end of the spectrum sit those who are open books, who believe in freedom of expression and think that those who advocate for greater privacy have something to hide. In the noted case, the court attempted to strike a balance between these two polar opposites and, with its decision, took a monumental step towards safeguarding Internet privacy. However, with great decisions come great consequences, and several implications stem from this decision.

The court in the noted cased expanded the scope of the Directive in more ways than one. The decision stretched the Directive's concept of a "controller" to include even those who serve as operators of search engines because they determine the purpose and means of the data processing.[117] This broadening of the definition makes one wonder if the language could also be interpreted to include even those who are merely users of search engines because they too have the ability to act as designators of purpose. Would a college student who used search engines to collect information and then posted his findings on social media be considered a "controller" of data? Could a teenager on Facebook who shared a link to a newspaper article, in an unaltered form, be forced to comply with the laws of the Directive? The implications of this kind of definitional stretch are endless.

The court continued to expand the application of the Directive with its vague interpretation of the activities that fall under the topic of "data processing."[118] The court danced around the argument made by Google Spain and Google Inc. that, as search engines, they merely display links in a list of search results and do not affect the selection between those sites that contain personal data and those that do not.[119] Furthermore, Google Inc. and Google Spain argued that even if their actions are to be considered data processing, because they do not have any knowledge regarding the displayed data, they do not possess the control that a typical "controller" would.[120] In response, the court merely presented a seemingly endless list of activities that could be considered "processing" under the Directive rather than directly addressing the argument.[121] The

117. *Id.* ¶ 33.
118. *Id.* ¶¶ 25-28.
119. *Id.* ¶ 22.
120. *Id.*
121. *Id.* ¶ 25.

provided list begs the question: What kind of activities are not subject to the Directive's control?

In its response to Google Inc.'s argument, the court reiterated the conclusion of *Satamedia*, explaining that even republishing data that has already been processed and made public is still an act of processing under the Directive.[122] Interestingly, the court skated past the subject of the obligations and requirements of an original data processor—the one who made that information available for republishing and reprocessing in the first place. The court only briefly touched upon this topic, falling back on the protective objectives of the Directive and concluded that, subject to the exceptions provided by the Directive, all data must comply with the provisions.[123] But what if the original data processing was done in violation of the Directive? Would a second processor still be liable for the first processor's crime? The court left these questions unaddressed, possibly choosing not to elaborate because the published information in the noted case was initially posted in accordance with the law.[124]

Furthermore, the court neglected to draw attention to the fact that the Directive was adopted in 1995, a time when technology was nowhere near as advanced and intricate as it is today. It is unlikely that the drafters of the Directive anticipated this kind of continuous widening because the invasiveness of technology was unforeseeable. The kind of controllers and data that the Directive was intended to target unlikely exist in today's society and their modern replacements are far from comparable. Consequently, the Directive now impacts people and information that it was not originally created to affect. However, it is likely that the drafters of the Directive predicted some type of modernization judging by the exceptions written into the Directive that establish safeguards to protect the rights of controllers and processors.[125] Therefore, even while the court expands data subject's privacy rights, the exceptions still preserve the right of freedom of expression.[126]

However, these negative implications seem immaterial and miniscule compared to one significant conclusion that stems from this decision. This is a decision of the CJEU, yet its affects a corporation headquartered in the United States. The decision made by the court does not just alter the behavior of the Member States in Europe, but it has the ability to affect those who are outside the court's jurisdiction. In the

122. *Id.* ¶¶ 30-31; *see also* Case C-73/07, *Satamedia*, 2008 E.C.R. I-9831, ¶¶ 48-49.
123. Case C-131/12, *Google Spain*, ¶¶ 66-71.
124. *Id.* ¶ 16.
125. *See supra* notes 19-21 and accompanying text.
126. *See supra* note 21 and accompanying text.

noted case, the court reasoned that when a parent company establishes a subsidiary or a different branch of their company in a Member State, that company makes itself vulnerable to the authority of EU laws.[127] So, although a controller is not subject to the provisions of the Directive unless its actions involve one of the Member States, the weight the court's decision carries is substantial. Most relevantly, the implications of this interpretation of the Directive enable the court to impose EU laws on non-EU companies, even if the controlling privacy laws in the country in which they are headquartered are in stark contrast to the EU's. This, coupled with the court's already broad interpretation of the Directive's terminology, results in an extremely expansive decision that has the possibility to affect an astonishing number of people, especially in a day and age where the use of the Internet is widespread.

Furthermore, it is noteworthy that the links González wished to be removed contained truthful information about his past that had since become irrelevant.[128] At this very moment, the Internet contains a considerable amount of information that could be deemed "inadequate, irrelevant or excessive."[129] It seems as though the next logical step in the court's decision-making process will be simply to order the erasure of all personal data on the Internet that has become incompatible with the Directive over time, thus avoiding further complex litigation and eliminating the inevitable cluttering of courts by plaintiffs alleging the existence of incompatible personal information on the Internet. Although this seems like a remote solution, the court's decision in the noted case paves the way for that kind of legislation. In fact, only a mere five months after the court's holding went into effect, Google Inc. reported that it had processed 143,000 requests related to 491,000 different links.[130] It is indubitable that those numbers will only grow as time goes on.

On the other hand, this expanding interpretation of the Directive can be viewed in a positive light because the court's decision enlarged the amount of protectable, personal data. In an age where privacy is practically a myth, the court's decision restored a citizen's power to keep some aspects of their life private. The decision gives people the ability to place an obstacle in the path of those who are trying to discover personal

---

127. *See supra* notes 84-89 and accompanying text.

128. Case C-131/12, *Google Spain*, ¶ 15.

129. *Id.* ¶ 92.

130. Mark Scott, *Google Provides Details on 'Right To Be Forgotten' Requests in E.U.*, N.Y. TIMES (Oct. 9, 2014, 7:00 PM), http://bits.blogs.nytimes.com/2014/10/09/google-provides-details-on-right-to-be-forgotten-requests/?_r=0.

information about them, thus enabling the censorship of sensitive, irrelevant information that has been made public. Though the court considers the seriousness of the interference into a data subject's private life and the potential harm the processing could cause, it has also held that an inconvenience is not necessary for a required removal.[131] This conclusion furthers the expansion of the amount of personal data that falls under the control of the Directive because it allows people to request the removal of information that is not necessarily harmful or offensive, just data that they do not want to be easily discovered. Though data must possess certain characteristics to be deemed incompatible with the Directive, it is clear that the court's interpretation is one aimed at making the Directive as all-inclusive as possible.[132] In light of the fundamental privacy rights of data subjects, this is a welcomed and progressive movement toward guaranteed privacy.

In this decision, though the court establishes a protective firewall safeguarding people's private information, the holding equally imposes a substantial impact on data processors. Critics complain that this interpretation elevates the privacy rights of private citizens, making them superior to the freedom of expression.[133] However, these critics ignore the exceptions provided in the Directive that ensure the majority of information remains untouched and uncensored. The "right to be forgotten" does not allow the erasure for all personal information on the Internet; rather, the court's interpretation merely tailors the Directive to be read in more modern terms.

Regardless, the question remains: Where does this "right to be forgotten" end? Evidently, the court has determined that those who have had financial issues in the past, like González, have a right to request the removal of that information once it becomes irrelevant, but how far does this privilege extend? Should those with criminal records be afforded the right to have information about their pasts removed postrehabilitation or after a substantial amount of time has passed, thus making their convictions "irrelevant"? Should search engines be developing preemptive programs that phase out and delete search result links that contain information as it becomes outdated with the passage of time? The court's conclusion regarding the broad range of the Directive's

---

131. Joined Cases C-465/00, 138/01 & 139/01, Rechnungshof v. Österreichischer Rundfunk, 2003 E.C.R. I-4989, ¶¶ 75, 89.

132. *See supra* notes 107-110 and accompanying text.

133. Roy Greenslade, *Article 19's Call to Google over 'Right To Be Forgotten' Ruling*, GUARDIAN (Oct. 16, 2014, 6:00 AM), http://www.theguardian.com/media/greenslade/2014/oct/16/freedom-of-speech-google.

applicability coupled with the vague language and descriptions in the opinion make the list of consequences seemingly and dangerously endless.

V. CONCLUSION

Modern technology is becoming increasingly intrusive. The world now contains phones that have the ability to track a person's every move, computers that can transcribe speech into typed documents, and websites that allow nearly anyone to edit displayed information. In a time where the right to privacy is slowly diminishing, the court in the noted case put its foot down in the interest of shrinking the ever-increasing amount of public information, and I do not see this being the end of data censorship and removal. It is foreseeable that the court will have to interpret the language of the Directive once again. Even in the noted case, which was decided less than a year ago, the court's explanations of its conclusions and definitions remain vague and open-ended. Judging by the precedent, the court's interpretations of the Directive follow a pattern of slowly increasing the amount of provided protection for data subjects. Hopefully, this pattern is a product of the realization that the Directive is a piece of legislation that was written over two decades ago, and its modern application is of growing concern.

It is my belief that the court start over with a clean slate. Clearly, the method of applying and interpreting a piece of legislation that was formulated with the purposes of protecting personal data when the Internet was brand new is not proving to be effective. The Internet is now one of the largest sources of information in the world. Because of this, it is highly probable that it contains the widest range of personal information on an almost unimaginable number of people. It would be in the best interest of the EU to start over, draft new legislation, and include provisions that specifically address Internet processing so that it does not have to readdress this ever-confusing and vague document every few years.

Sarah M. Kalis*

 J.D. candidate 2016, Tulane University Law School; B.S. 2012, Florida State University. Sarah would like to thank her family, friends, and the members of the Journal for all their help, support, and endless patience.