



Digital Commons@
Loyola Marymount University
LMU Loyola Law School

Loyola of Los Angeles International and Comparative Law Review

Volume 38 | Number 2

Article 1

Fall 2016

European Data Protection Uncapped: A Critical Analysis of Google Spain v. AEPD

Adam Byrne

Follow this and additional works at: <https://digitalcommons.lmu.edu/ilr>



Part of the [Comparative and Foreign Law Commons](#), and the [International Law Commons](#)

Recommended Citation

Adam Byrne, *European Data Protection Uncapped: A Critical Analysis of Google Spain v. AEPD*, 38 Loy. L.A. Int'l & Comp. L. Rev. 115 (2024).

Available at: <https://digitalcommons.lmu.edu/ilr/vol38/iss2/1>

This Article is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles International and Comparative Law Review by an authorized administrator of Digital Commons@Loyola Marymount University and Loyola Law School. For more information, please contact digitalcommons@lmu.edu.

European Data Protection Uncapped: A Critical Analysis of Google Spain v. AEPD

ADAM BYRNE

I. INTRODUCTION

In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (hereinafter “*Google Spain*”), the European Court of Justice held that Google, as the operator of an internet search engine, must remove a person’s name from a list of its search results at the request of that person.¹ The information related to the person need not be prejudicial to him or her; their individual right to have that information stricken from the list of search results overrides both the economic interests of the search engine and the general public’s interest in having access to that information.² A minor but ill-defined exception is made, however, for people who, because of the role they play in public life, have their individual rights trumped by the general public’s interest in access to their information.³

This comment will first summarize the factual and procedural history of the case, followed by a more detailed description of the court’s reasoning and ultimate holding. This comment will then demonstrate how this case was incorrectly decided by closely examining three mistakes that the court made. First, the court misinterprets Directive 95/46 by giving Article 6(1) more force than it merits.⁴ Second, the court highlights Articles 7 and 8 of the Fundamental Rights Charter while paying no heed to Article 11, which specifically provides for the freedom of

1. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

2. *Id.* ¶ 100(4).

3. *Id.*

4. *See generally, id.* ¶ 71.

expression.⁵ Third, the court only causes more confusion as to which types of information are susceptible to removal and which types are not. This comment will finish with a discussion of both the positive and negative ramifications that the decision will likely have in the years to come.

II. STATEMENT OF THE CASE

A. Factual Background and Procedural History

The European Court of Justice (hereinafter “ECJ” or “Court”) rendered its decision of *Google Spain* on May 13, 2014.⁶ The case involved Mr. Mario Costeja González, a resident of Spain, who wanted to keep information about himself out of the public’s reach.⁷ In 1998, Mr. González appeared in a real-estate auction connected with attachment proceedings for the recovery of social security debts.⁸ *La Vanguardia*, a popular Spanish newspaper, published two articles related to this auction.⁹ These articles were preserved on the newspaper’s website and could be accessed by any internet user entering Mr. González’s name into Google’s search engine.¹⁰ According to Mr. González, the attachment proceedings he was involved in had been resolved many years in the past and were no longer relevant in any way.¹¹

In order to block that information and prohibit the public from accessing it, Mr. González filed a complaint with the *Agencia Española de Protección de Datos*¹² (hereinafter “AEPD”). The AEPD is an independent public law authority that oversees compliance with the European legal provisions on the protection of personal data.¹³ Much like its counterparts in other European countries, the AEPD is essentially an agency assigned to administer, interpret, and apply the European Union’s legal framework for data protection.¹⁴

5. See generally, *id.* ¶ 97.

6. See generally Case C-131/12.

7. See generally *id.* ¶ 71.

8. *Id.* ¶ 14.

9. *Id.*

10. *Id.*

11. Case C-131/12 ¶ 15.

12. *Id.* ¶ 15.

13. SPANISH DATA PROTECTION AGENCY, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/AEPD_en.pdf.

14. *Id.*

Mr. González made two different requests to the AEPD. First, he sought to enjoin *La Vanguardia* from maintaining the personal information relating to him.¹⁵ Second, he asked that Google be forced to alter their search engine so that a search of his name would not show an internet user the links to the newspaper's website.¹⁶

On July 30, 2010, the AEPD issued its ruling.¹⁷ It rejected Mr. González's first request on the grounds that *La Vanguardia* published the auction information as required by the Ministry of Labour and Social Affairs.¹⁸ The Ministry had apparently ordered the information be published as a way to garner publicity for the auction and attract the attention of bidders.¹⁹ As for the second request, however, the AEPD ruled in favor of Mr. González and ordered Google to stop including the pertinent newspaper pages in their search results.²⁰ Given its obligation towards an individual's fundamental right to data protection, the AEPD felt that it was justified in requiring search engine operators like Google to remove the data and prevent access to it.²¹

Both Google Inc. and Google Spain filed separate lawsuits in the Audiencia Nacional, a Spanish high court, to challenge the AEPD decision.²² After joining the two suits, the court stayed the proceedings and referred several critical questions to the ECJ for a preliminary ruling.²³ The underlying reason behind this request for clarification was that the applicable law, namely, the 1995 EU Data Protection Directive 95/46²⁴ (hereinafter "Directive 95/46" or "Directive"), was drafted before internet search engines became widespread. The AEPD, therefore, asked for the ECJ's interpretation of Directive 95/46 as it applies to search engines.

There were three main issues presented to the ECJ. First, the AEPD was unsure about whether Directive 95/46 controls in this case given the fact that Google is a corporation that conducts its search en-

15. Case C-131/12 ¶ 15.

16. *Id.*

17. *Id.* ¶ 16.

18. *Id.*

19. *Id.*

20. Case C-131/12 ¶ 17.

21. *Id.*

22. *Id.* ¶ 18.

23. *Id.* ¶ 20.

24. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046>.

gine operations outside of Spain.²⁵ Second, if Directive 95/46 does indeed control, there is the issue of whether its provisions are even applicable to search engine operators like Google.²⁶ Lastly, the AEPD asked whether data subjects like Mr. González can invoke Directive 95/46 to compel the operator of an internet search engine to block and erase information relating to him.²⁷

B. The ECJ's Holding

As to the first issue regarding the territorial scope of Directive 95/46, the ECJ held that Google does indeed fall within its parameters.²⁸ To arrive at this conclusion, the Court specifically looked at the definition of the term "establishment" within the meaning of Article 4(1)(a) of the Directive.²⁹ Google Inc. argued that Google Spain is not an "establishment" because it was not involved in the company's search engine operations.³⁰ Mr. González, on the other hand, argued that there was an "inextricable link" between Google Spain and Google Inc.'s search engine activity.³¹ Although Google Spain does not collect or index information, one of its main functions is promoting and selling advertising space offered by the search engine in order to make it profitable.³²

In addition to these competing arguments, the Court considered the Directive's preamble, which states, in pertinent part, that "establishment . . . implies the effective and real exercise of activity through stable arrangements."³³ Here, Google Spain indisputably engages in such activity through arrangements with Google Inc. Moreover, the Court mentioned how the Directive does not require the actual processing of data to be carried out "by" the establishment; all that matters is that the data processing is carried out "in the context of the activities" of the establishment.³⁴ These findings led the Court to its conclusion that Google Spain is considered an "establishment" for purposes of the Directive.³⁵

To resolve the second issue over the Directive's potential applica-

25. Case C-131/12 ¶ 20.1.

26. *Id.* ¶ 20.2.

27. *Id.* ¶¶ 72, 76.

28. *Id.* ¶ 59.

29. *Id.* ¶ 45.

30. Case C-131/12 ¶ 47.

31. *Id.*

32. *Id.* ¶ 55.

33. Council Directive 95/46/EC, *supra* note 24, ¶ 19.

34. *Id.* ¶ 52.

35. *Id.* ¶ 49.

bility, the Court analyzed whether Google Inc.'s search engine activity constitutes the "processing of personal data" under the Directive, and, if so, whether Google Inc. must be regarded as a "controller" under the Directive.³⁶ As to the first inquiry, Google argued that its activities ought not be considered the "processing of personal data."³⁷ The data appears on third party web pages and Google indexes all of the information regardless of the data being personal.³⁸ With respect to the second inquiry, Google contended that it cannot be a "controller" of the data when it has no knowledge of it, let alone no control over it.³⁹ Mr. González, however, was of the opinion that Google is engaged in the "processing of personal data" and that it amounts to a "controller" because it determines the objectives and techniques of its processing.⁴⁰

The Court relied on Article 2(b) of the Directive, which defines the "processing of personal data" as "any operation . . . performed upon personal data . . . such as collection, . . . retrieval, . . . use, . . . disclosure, . . . or otherwise making [it] available."⁴¹ In light of the fact that Google Inc.'s search engine collects, uses, and makes available personal information it finds already published on the internet, the Court held that Google Inc. is engaged in the "processing of personal data."⁴² In terms of whether Google Inc. constitutes a "controller," Article 2(d) of the Directive defines "controller" as the "legal person . . . or any other body which . . . determines the purposes and means of the processing of personal data."⁴³ Search engine operators, the Court reasoned, do in fact determine the purpose and means of processing data.⁴⁴ Thus, using the definition set forth in Article 2(d), the Court found no trouble in coming to the conclusion that Google Inc. is a "controller" under the Directive.⁴⁵ The Court supported this finding by stressing how search engines, by virtue of their activity, significantly affect a data subject's fundamental right to protect personal information and therefore have the responsibility to ensure that the requirements of the Directive are met.⁴⁶ Given that Google Inc. not only "processes per-

36. *Id.* ¶ 21.

37. *Id.* ¶ 47.

38. Council Directive 95/46/EC, *supra* note 24, ¶ 22.

39. *Id.*

40. *Id.* ¶ 23.

41. Council Directive 95/46/EC, *supra* note 24, at art. 2(b).

42. Case C-131/12 ¶ 28.

43. Council Directive 95/46/EC, *supra* note 24, at art. 2(d).

44. Case C-131/12 ¶ 33.

45. *Id.*

46. *Id.* ¶ 38.

sonal data,” but is also the “controller” of such activity, the provisions of the Directive are fully applicable to its actions.

The final issue presented to the ECJ was whether search engine operators are obliged to remove personal data at the request of the data subject. In pleading its case, Google Inc. suggested that any burden of removal should be passed on to the publisher of the website concerned.⁴⁷ After all, that is where the personal data is originally made public and where it can most effectively be removed.⁴⁸ In addition, Google Inc. claimed that requiring it to remove the information from its indexes would ignore the rights of those who publish websites as well as those who wish to access that information.⁴⁹ Mr. González, though, asserted that a national authority, in this case, the AEPD, can require search engine operators to withdraw personal information even though that information was lawfully published on the original website.⁵⁰

In addressing this issue, the Court first expressed its obligation to interpret the Directive in the light of the E.U.’s Charter of Fundamental Rights (hereinafter “Charter”).⁵¹ The relevant portions of the Charter in this case are Article 7, which protects the right to privacy, and Article 8, which guarantees the right to protect one’s personal data.⁵² The Directive and the Charter, taken together, ensure a high level of protection is given to individuals over their own personal information. Next, the Court examined specific provisions of the Directive. For example, Article 12(b) states that data subjects have the right to demand the controller to rectify, erase, or block personal data, especially if such information is inaccurate.⁵³ The Court also looked to Article 14(a), which prescribes the data subject’s right to object “on compelling legitimate grounds.”⁵⁴ With the foregoing provisions in mind, the Court held that the operators of search engines are obliged to remove from their list of results any link to a data subject’s name in order to comply with the Directive.⁵⁵

In sum, the ECJ’s three main findings amounted to a significant decision in favor of the AEPD and Mr. González. Google and similar search engine operators will now have to remove personal information

47. *Id.* ¶ 63.

48. *Id.*

49. Case C-131/12 ¶ 63.

50. *Id.* ¶ 65.

51. *Id.* ¶ 68.

52. Charter of Fundamental Rights of the European Union, art. 7-8, 2000 O.J. (C 364) 1, 10.

53. Council Directive 95/46/EC, *supra* note 24, at art. 12(b).

54. *Id.* at art 14(a).

55. Case C-131/12 ¶ 88.

from their search results at the request of individuals who no longer wish such information to be publicly accessible. There was, however, one caveat to the Court's ruling: there may be times when the public has a greater interest in access to information about an individual because of their role in public life or other "particular reasons."⁵⁶ Although this exception remains ill-defined, the decision still stands as having a remarkable impact on European internet use.

III. THE ECJ'S THREE FATAL MISTAKES

A. Misinterpretation of Directive 95/46

The ECJ made several critical errors in its analysis of the case and the consequences of these mistakes will likely prove to be costly in the future. One such error was the Court's misinterpretation of Directive 95/46. As stated above, the Court held that Google Inc. ought to be considered a "controller" because it "determines the purposes and means of the processing of personal data."⁵⁷ The Court's reasoning here is weak and unconvincing. Yes, Google Inc. does determine the purposes and means of the processing of data, but Google Inc. does not determine as much with regard to *personal* data. In his advisory opinion, Advocate General Jääskinen expressed his doubt as to whether Google Inc. was a "controller" when its objective consists of processing files that contain personal information as well as files containing other, non-protected data in "a haphazard, indiscriminate, and random manner."⁵⁸ To further elaborate this concern, he stated:

"In my opinion the general scheme of the Directive . . . [is] based on the idea of *responsibility of the controller* over the *personal* data processed in the sense that the *controller* is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their processing as personal data."⁵⁹

In other words, an internet search engine must exercise real control over the personal data it processes for it to constitute a "controller" under the Directive. Google Inc.'s search engine activities involve com-

56. *Id.* ¶ 97.

57. Council Directive 95/46/EC, *supra* note 24, at art. 2(d).

58. Case C-131/12, Opinion of Advocate General Jääskinen, *Google Spain SL v. Agencia Española de Protección de Datos*, 2013 E.C.R. I-424, ¶ 81.

59. *Id.* ¶ 82.

puter-coded crawlers that automatically retrieve and copy website information.⁶⁰ In carrying out this operation, Google Inc. is not aware of the existence of personal information aside from the statistical likelihood that personal data is inscribed somewhere on the webpage that is being collected and indexed.⁶¹ Google Inc. merely provides an informational tool to help others access the personal data that has originated from third-party websites, far removed from its own control.

In an attempt to strengthen its conclusion, the Court points out that Google Inc. plays a “decisive role” in the dissemination of the personal data, making it accessible to “internet users who otherwise would not have found the web page on which those data are published.”⁶² This assertion, however, is demonstrably false. For example, imagine that the current owner of the real estate previously belonging to Mr. González wishes to know more information about the previous owners of the property. The owner could simply go to the website of *La Vanguardia*, briefly search through its archives and arrive at the same website pages Mr. González seeks to have erased. Google Inc. may facilitate this process, but the plain fact that this can all be done without the use of Google’s search engine undermines the Court’s position that Google Inc. is a “controller” and thereby questions the Directive’s applicability in this case.

The final pillar upon which the Court rests its conclusion also fails to stand. The Court mentions the general purpose of the Directive and reiterates that it aims to ensure the “effective and complete protection of data subjects.”⁶³ Therefore, it argues, Google Inc. must be considered a “controller,” especially in light of the protection provisions codified in the Charter.⁶⁴ By blanketing its reasoning with references to the broad and admirable goals of the Directive and the Charter, the Court insufficiently covers up its conclusory assertions, for the Court’s reliance on these broad principles of data protection have nothing to do with Google’s status as a “controller.”

B. Myopic Reading of The Charter of Fundamental Rights

In reaching its decision in favor of the AEPD and Mr. González, the ECJ interprets the provisions of the Directive in the light of Articles

60. *Id.* ¶ 86.

61. *Id.* ¶ 84.

62. Case C-131/12 ¶ 36.

63. *Id.* ¶ 38.

64. *Id.* ¶ 41.

7 and 8 of the Charter. Article 7, as previously stated, guarantees an individual's right to privacy,⁶⁵ while Article 8 describes an individual's right to protect personal data.⁶⁶ These rights are alluded to numerous times throughout the Court's opinion,⁶⁷ each time stressing the significant amount of protection that the current European legal regime affords data subjects. Surprisingly, the Court omits any reference to Article 11 of the Charter, which guarantees the freedom of expression and information.⁶⁸

The notion that one has a right to protect their own private information while one also has a right to express themselves freely creates a set of conflicting interests. *Google Spain* is a prime example. Mr. González had an interest in controlling his personal data while *La Vanguardia* had an interest in publishing that data. One of the cornerstones of the Court's decision was its emphasis on the Charter. However, it only explores the ramifications of Articles 7 and 8. Article 11, meanwhile, goes unmentioned.

A comparison of the articles found in the Charter reveals some telling signs that the Court took an erroneous approach to this set of conflicting interests. Article 11 states that, "[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."⁶⁹ This language is stated in a very broad and straightforward fashion. It describes the right to freely express ideas as if it should always be held in the highest regard. Article 11 even goes so far as to preclude interference by public authority to protecting the freedom of expression and information.

Article 8, on the other hand, deals with the right to protect personal data. There are two pertinent sections in Article 8. Section 1 states that "[e]veryone has the right to the protection of personal data concerning him or her."⁷⁰ In applying this section to *Google Spain*, it must be made clear that the article describes the right to "protect" personal data, not

65. Charter of Fundamental Rights of the European Union, *supra* note 52, at 10. *See also* Case C-131/12 ¶ 41.

66. "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." *Id.* at art. 8.

67. Case C-131/12 at ¶¶ 1, 69, 74, 81, 97, and 99.

68. Charter of Fundamental Rights of the European Union, *supra* note 52, at art. 11.

69. *Id.*

70. *Id.* at art. 8.

the right to “control” it.⁷¹ Whether controlling information is a form of “protection” has not yet been answered and is something that the Court should have looked at more closely before reaching its decision.

Section 2 can be broken down into two separate clauses. Clause 2 states that “[s]uch data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.”⁷² While Mr. González did not give his consent to Google collecting and indexing his personal information, Google still had a legitimate basis under Article 11 to collect this publicly available personal data and freely express itself by making the information accessible on its search engine. Clause 2 states that “[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”⁷³ Here, Mr. González certainly had access to the collected data. All he needed to do was type his name into Google’s search engine. The real issue is whether his request to have that data taken down falls under his right to “rectify” his personal information. To “rectify” means to “set something right; to correct something.”⁷⁴ The personal information relating to Mr. González that was on *La Vanguardia*’s website and made more accessible through Google’s search engine was not inaccurate, mistaken or erroneous by any measure. Therefore, the data was incapable of being rectified. This argument is further supported by reference to Article 12(b) of Directive 95/46, which states that a data subject has the right to obtain from the controller “the rectification, erasure, or blocking of data . . . in particular because of the incomplete or inaccurate nature of the data.”⁷⁵ Again, the data involved in this case was neither incomplete nor inaccurate. To have this information taken down at the request of Mr. González would not be correcting any falsities made about him nor would it be setting anything right. Rather, it would be his way of making accurate personal data no longer widely available to the public simply because he does not want others to know about it. It appears, then, that Article 8 does not have as great an impact on this case as the Court’s decision implies.

Unlike Article 8, Article 11 is directly applicable to *Google Spain* and merits much more attention. The Court dismisses this position by

71. *Id.*

72. *Id.*

73. Charter of Fundamental Rights of the European Union, *supra* note 52, at art. 8.

74. THE AMERICAN HERITAGE COLLEGE DICTIONARY 1164 (4th ed. 2004).

75. Council Directive 95/46/EC, *supra* note 24, at art. 12(b).

suggesting that search engine operators do not engage in any form of expression.⁷⁶ In making this judgment, the Court looks to Directive 95/46, which directly addresses the conflicting interests between one's protection over their personal data and one's freedom of expression.⁷⁷ According to the Directive, derogations from its provisions shall be provided for "the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."⁷⁸ The Court interpreted the activities of Google as not being carried out solely for journalistic purposes and therefore held it was not exempt from the provisions of the Directive.⁷⁹

Underlying the Court's reasoning is a very narrow view of what constitutes expression. The Court forgets to mention that the Directive's exceptions also apply to processing done for the purpose of artistic or literary expression.⁸⁰ When companies such as Google provide internet search engine services, they are in fact exercising their freedom of expression, albeit subtly, in an artistic manner.⁸¹ The lists of results that are displayed in a Google search reflect an expression that "these are the relevant search results."⁸² The layout and design of its search engine are also expressive. Google is well known for its daily "doodles" that creatively attract attention to people, events, and ideas that it deems important. Just because these expressions are subtle and made in a digital format should not detract from them the protection they ought to enjoy.⁸³

Along with search engine operators, individual website publishers will also have their freedom of expression encroached upon by the ECJ's decision. The Court distinguishes individual website publishers from search engine operators by asserting that a search engine operator is "liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."⁸⁴ In the Court's view, search engines like Google play a "deci-

76. Case C-131/12 ¶ 85.

77. Council Directive 95/46/EC, *supra* note 24, ¶ 49.

78. *Id.* at art. 9.

79. Case C-131/12 ¶ 85.

80. Council Directive 95/46/EC, *supra* note 24, at art. 9.

81. Case C-131/12, Opinion of Advocate General Jääskinen, *supra* note 58, ¶ 132.

82. Allyson Haynes Stuart, *Google Search Results: Buried if Not Forgotten*, 15 N. CAROLINA J. L. & TECH. 463, 488 (2014).

83. *Id.*

84. Case C-131/12 ¶ 87.

sive role” in distributing the data, making it more accessible and enabling internet users to more easily establish a detailed profile of the data subject.⁸⁵ The Court’s analysis here focuses on the concerns of data subjects and their right to privacy, but no consideration is given to the website publishers and their freedom of expression. While website publishers remain free to post content on their web pages, the size of the audience that they can reach through search engines is significantly diminished. Legitimate information that has entered the public sphere is ultimately censored by a private individual.⁸⁶

Although quickly dismissed by the Court, an individual’s freedom of expression is one of their most precious rights.⁸⁷ Recent events in France can attest to this. On January 7, 2015, two masked gunmen slaughtered twelve individuals in an attack on the Parisian satirical magazine *Charlie Hebdo*.⁸⁸ The massacre was believed to have been inspired by publications of the magazine featuring controversial illustrations of the Prophet Mohammed.⁸⁹ In response to this tragedy, hundreds of thousands of people gathered in Paris to rally against terrorism and stand up for their freedom of expression.⁹⁰ While it is not the purpose of this comment to argue that free speech should be unfettered, it should be recognized that legally protected speech that is published onto a website deserves the fullest protection of the law and should not be made less accessible by the wishes of a discontented data subject.

In *Google Spain*, the Court does briefly refer to the “legitimate interest of internet users potentially interested in having access” to personal data.⁹¹ The right of the public to access information could be considered a logical extension of one’s freedom of expression. The Court attempts to resolve the conflict between an internet user’s interest and a data subject’s rights by suggesting that a “fair balance” be sought.⁹² The practical consequences of balancing these interests on a case-by-case basis, however, are not yet clear.⁹³ What is clear, though, is that an in-

85. *Id.* ¶¶ 35-37.

86. Case C-131/12, Opinion of Advocate General Jääskinen, *supra* note 58, ¶ 133.

87. *Id.*

88. *Charlie Hebdo Attack: Three days of terror*, BBC NEWS (Jan. 14, 2015), <http://www.bbc.com/news/world-europe-30708237>.

89. Nick Thompson, *Charlie Hebdo: Satirical magazine is no stranger to controversy*, CNN (Jan. 7, 2014), <http://edition.cnn.com/2015/01/07/europe/charlie-hebdo-controversy/>.

90. Ashley Fantz, *Array of world leaders joins 3.7 million in France to defy terrorism*, CNN (Jan. 12, 2014), <http://edition.cnn.com/2015/01/11/world/charlie-hebdo-paris-march/>.

91. Case C-131/12 ¶ 81.

92. *Id.*

93. See Case C-131/12, Opinion of Advocate General Jääskinen, *supra* note 58, ¶ 133 (“I

ternet user's right to access information would be compromised if his online search of an individual generated only a censored list of web pages as opposed to a relevant list.⁹⁴

C. Providing an Unclear Exception

The Court firmly stands behind its general rule that the interests of internet users are overridden by a data subject's right to privacy and protection.⁹⁵ An exception is made, however, in particular cases where the interference with a data subject's privacy rights are justified by the preponderant interest of the general public in having access to the information through a list of search results.⁹⁶ To give an example, the Court cites that the role played by the data subject in public life may satisfy the criteria for an exception to its general rule.⁹⁷ A famous businessman or an important political figure may meet this standard if the public's interest in having information about them is greater than their own privacy interests.

There is certainly some logic to be found in this exception. The prime minister of a nation, for instance, cannot reasonably expect that their interest in keeping all of their information private outweighs the interest of the public who deserves access to that information. The prime minister throws himself or herself into the limelight by campaigning for the position and being elected. Being subjected to public investigation and criticism is part of the job. By the same token, a prime minister can reasonably expect that his interest in keeping things like his bank account number and his computer password private greatly outweigh the public's interest in accessing that information.

As this example illustrates, there are a multitude of variables that need to be taken into consideration when finding the "fair balance" that the Court describes. The error in the Court's reasoning is that the balance is not "fair" by any means. The Court even admits that, as a general rule, the data subject's rights override the interests of the general public.⁹⁸ Treating the right to privacy as presumptively superior to the right of accessing information stands as a serious affront to the freedom

would also discourage the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis.").

94. *Id.* ¶ 131.

95. Case C-131/12 ¶ 81.

96. *Id.* ¶ 97.

97. *Id.*

98. *Id.*

of expression. The Court fails to explain why information that is legally published on a website is no longer legally protected once collected and indexed by a search engine. Without lending any guidance in its opinion, the Court in *Google Spain* leaves too much room for arbitrary decision-making by judges faced with similar questions. The exception to the general rule is so ill defined that eventually it will cease to have any effect. Whether a data subject's role in public life makes their personal data so sensitive that it outweighs the public's interest in accessing that information will be determined solely by the predilections of sitting judges.

IV. CONSEQUENCES OF *GOOGLE SPAIN*: A POLICY PERSPECTIVE

A. *The Winners*

First and foremost, *Google Spain* stands as a major victory for advocates of privacy and data protection. Many commentators have praised the decision as a proper step towards the preservation of an individual's right to privacy and the recognition that people ought to be able to exercise control over their personal information.⁹⁹

These sentiments, it should be noted, are not novel. In fact, the right to privacy has been established and supported for many years. In their seminal 1890 law review article "The Right to Privacy," Samuel D. Warren and Louis D. Brandeis set forth a number of arguments why the law must fully protect one's privacy rights.¹⁰⁰ The article cites examples of newspapers invading the privacy of individuals, subjecting them to "mental pain and distress far greater than could be inflicted by mere bodily injury."¹⁰¹ The article was even prophetic of the events that took place in *Google Spain*. It referred to "numerous mechanical devices" that would be able to make "what is whispered in the closet . . . proclaimed from the house-tops."¹⁰² To counter this threat, the article suggests that the law must afford some remedy for the "unauthorized circulation of portraits of private persons."¹⁰³

"[I]t is hard to overstate the importance of protecting personal da-

99. Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html.

100. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

101. *Id.* at 196.

102. *Id.* at 195.

103. *Id.*

ta.”¹⁰⁴ Informational privacy, however, is an “evolving concept.”¹⁰⁵ With the advent of the internet and the proliferation of accessible data, one’s right to control what is being said about them online has been dubbed by many as “The Right to be Forgotten.”¹⁰⁶ This right has been given various meanings. One such interpretation is that the right to be forgotten involves “the right to have personal information migrate from a public or disclosed sphere to a private or limited access sphere.”¹⁰⁷ Others describe the right as “an individual’s right to control and possibly delete personal information about herself in the hands of others, usually because that information is outdated or no longer relevant.”¹⁰⁸ Still others posit that the right to be forgotten is “not a right to be purged from the memory of people who know you, but rather to control how information about you appears online.”¹⁰⁹ While these definitions differ in one way or another, they all point to the same general principle: one’s right to privacy extends to one’s ability to control access to their personal information.

The intrinsic value of the right to be forgotten can be found by simply imagining the world without it. If the internet was left completely unregulated and search engines operated without restraint, people would find themselves in uncomfortable and vulnerable positions. Given their immense popularity, internet search engines like Google have “the power to make or break someone’s personal or professional reputation.”¹¹⁰ A single mistake or scandal in someone’s life might show up at the top of results after a search of a person’s name, forever stigmatizing them and defining who they are to others.¹¹¹ This is especially troublesome considering how frequently employers and universities conduct internet searches when reviewing a pool of applicants.¹¹²

104. John Schinasi, Note, *Practicing Privacy Online: Examining Data Protection Regulations Through Google’s Global Expansion*, 52 COLUM. J. TRANSNAT’L L. 569, 570 (2014).

105. Meg Leta Ambrose, *It’s About Time: Privacy, Information Life Cycles, and the Right to be Forgotten*, 16 STAN. TECH. L. REV. 369, 374 (2013).

106. Posner, *supra* note 99.

107. Ambrose, *supra* note 105, at 375.

108. Stuart, *supra* note 82, at 465.

109. Evan Selinger & Woodrow Hartzog, *Google Can’t Forget You, But it Should Make You Hard to Find*, WIRED (May 20, 2014), <http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/>.

110. Stuart, *supra* note 82, at 477.

111. Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW U. L. REV. 105 (2010).

112. Stuart, *supra* note 82, at 477 (“Recent surveys found that 79% of employers and 40% of law schools search for information about their applicants by using the internet.”).

The dangers that would be present in a world where people lack control over their own personal data are numerous, harmful, and scary. There are many categories of information that, in the interest of everyone, simply should not be made public. These include bank accounts, credit card numbers, and information relating to minors.¹¹³ If these types of information are leaked or uploaded in an unauthorized fashion, a remedy needs to be made available so that individuals can address the problem and stop the bleeding. There are many recent examples of what happens when information is left unchecked on the internet. One man was stalked by an ex-girlfriend who uploaded private photos and posted defamatory comments about him, calling him a psychopath and a child molester.¹¹⁴ An alarming number of cases involving “cyber-bullying” have also come up in recent years. Minors can and have been abusing social media to ridicule and demean their peers, causing anxiety, depression, and even suicide.¹¹⁵

In light of all the hazards that accompany free-flowing, widely accessible information, it is easy to see how important one’s right to privacy and data protection truly is. Germany, having the tightest data restrictions in Europe, appears to have taken the lead among E.U. members in the overall effort to defend and preserve this treasured right.¹¹⁶ It has clashed with Google for the past several years, suing the company in lawsuits over copyright infringements and anti-trust violations.¹¹⁷ Germany’s own Günther Oettinger, who was recently appointed as the European Commissioner for the Digital Economy, has been promulgating various anti-Google ideas and spreading his sentiments across all of Europe.¹¹⁸ This, along with the principles of the Directive and Articles 7 and 8 of the Charter, reflects a tidal wave of opposition that could potentially drown Google’s chances of operating successfully within the European marketplace.

B. The Losers

The ECJ’s decision in *Google Spain* inflicted a significant blow to

113. *Id.* at 468-69.

114. *Id.* at 478.

115. See generally Matthew C. Ruedy, *Repercussions of a Myspace Teen Suicide: Should Anti-Cyberbullying Laws be Created?*, 9 N. C. J. L. & TECH. 323 (2008).

116. Chase Gummer & Frances Robinson, *New EU Digital Chief Floats Tough Anti-Google Regulation*, WALL ST. J. (Oct. 30, 2014), <http://blogs.wsj.com/digits/2014/10/30/new-eu-digital-chief-floats-tough-anti-google-regulations/>.

117. *Id.*

118. *Id.*

Google and its operations as an internet search engine.¹¹⁹ The consequences of losing this lawsuit are significant and patently painful.¹²⁰ Google is now saddled with the obligation of granting the requests of thousands of Europeans who wish to have their personal information concealed and removed from the list of search results.¹²¹ An entire team of content supervisors now has to be created in order to receive and process tens of thousands of requests.¹²² Financially, a substantial amount of money must be spent in order to fund the handling of this burdensome workload.

In an insightful article published in *The New Yorker*, legal analyst Jeffrey Toobin describes the administrative system that Google was forced to institute in order to comply with the ECJ's ruling.¹²³ After interviewing David Price, one of Google's lawyers in charge of this undertaking, Toobin gives the following description:

To decide whether to remove the disputed links from its searches, Google has assembled dozens of lawyers, paralegals, and others to review the submissions. Price meets with the group twice a week to discuss its decisions and to try to maintain consistent standards. The main considerations are whether the individual is a public or a private figure; whether the link comes from a reputable news source or government Web site; whether it was the individual who originally published the information; and whether the information relates to political speech or criminal charges. Because the Court's decision specifically said that a relevant factor should be 'the role played by the data subject in public life, Google is reluctant to exclude links about politicians and other prominent people.¹²⁴

Toobin goes on to suggest that many of these decisions are "hard calls."¹²⁵ Operating under the threat of hefty fines, Google's content supervisors are more likely to err on the side of caution and remove the contested link than they are likely to keep the link where it is and risk further litigation. This unfortunate consequence deepens the wound that

119. See generally Sam Schechner, *Google Grants Majority of 'Right to be Forgotten' Requests*, WALL ST. J. (July 24, 2014), http://www.wsj.com/articles/google-grants-more-than-half-of-right-to-be-forgotten-requests-processed-so-far-1406223241?mod=yahoo_hs.

120. *Id.*

121. *Id.*

122. *Id.*

123. Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sept. 29, 2014), <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion>.

124. *Id.*

125. *Id.*

the ECJ's decision has inflicted on an individual's freedom of expression.

Unfortunately for Google, the onus does not stop there. Under the EJC's ruling, it is now incumbent upon Google that it limits its ability to tell the world what it finds to be the most popular web pages and what it considers to be the most relevant information. Furthermore, the burden Google now carries on its back extends to other internet search engines as well. Companies like Yahoo! and Bing will have to comply with the requirements because they too are "controllers" engaged in the "processing of data" under the ECJ's interpretation of those terms.

Although this landmark decision may appear to be a triumph for European citizens, they too suffer a tremendous loss at the hands of the ECJ by having their freedom of expression treaded upon. Reporters and journalists, for example, must be wary that when they publish an article online, there is a chance that an individual named in the article may not be so fond of what was written. The individual could then file a request for removal, thereby destroying the likelihood that an interested internet user could access that information by means of a search engine. Bloggers, photographers, and musicians are also subjected to the same risk of having their works suppressed at the will of an angry or discontented individual. People afraid of having their expressions removed will hesitate to upload them in the first place. This chilling effect caused by the ECJ's decision could soon result in a "climate of censorship."¹²⁶

Even Mr. González, the man who won his case against Google, will end up losing because he, along with all other Europeans, will now find it more difficult to access information online. According to Eurostat, the European Union's official statistics bureau, the number of Europeans who regularly use the internet has doubled since 2006.¹²⁷ Clearly, more and more Europeans are relying on the internet to provide them with the information they seek. The vast majority of these users opt for Google, a company which enjoys more than 90% share of the European internet search market.¹²⁸ The stringent requirements that the ECJ now places on Google will almost certainly frustrate many internet users and prevent them from acquiring data that they otherwise would have been able to access.

126. Stuart, *supra* note 82, at 482.

127. Mark Scott, *Europe's Internet Use Surges*, N.Y. TIMES (Dec. 16, 2014), http://bits.blogs.nytimes.com/2014/12/16/europes-internet-use-surges/?_r=0.

128. Matt Rosoff, *Here's How Dominant Google is in Europe*, BUSINESS INSIDER (Nov. 29, 2014), <http://www.businessinsider.com/heres-how-dominant-google-is-in-europe-2014-11>.

Finally, even Europe's data protection agencies come out as losers in the wake of *Google Spain*. Although the ECJ's decision involved Spain's data protection agency, it sets an important precedent for similar agencies in other European countries. Different countries have various traditions and legal norms, causing them to draw the line on internet issues in different ways.¹²⁹ This creates particular problems in the borderless world of the internet because the approaches taken by each country often times conflict.¹³⁰ For example, Germany is a nation that places great value on an individual's right to data privacy and it is likely to welcome the result of this case with open arms.¹³¹ In fact, a recent survey revealed that 97% of Germans believe that the misuse of personal data should be better tracked and more strongly penalized.¹³² The United Kingdom, on the other hand, is generally perceived to be more industry-friendly and, in some European eyes, it provides the weakest protection for personal data.¹³³ The ECJ's ruling conflicts with the UK's own data privacy laws, which will now have to be reassessed and perhaps amended in spite of local policies and practices.

The drafters of Directive 95/46, which mandated the creation of these data protection agencies, were cognizant that conflicts like this were likely to arise. To address the issue, the Directive required that the agencies maintain an independent status.¹³⁴ The importance of preserving impartiality was reaffirmed in 2012 when the ECJ held that Austria's data protection agency was acting in contravention of Directive 95/46.¹³⁵ According to the ECJ, Austria had enacted national legislation which prevented its data protection agency from exercising its functions

129. Toobin, *supra* note 123.

130. *Id.*

131. Alison Coleman, *Germany's Security Startups Leading a Global Demand for Online Data Privacy*, FORBES (Oct. 1, 2014), <http://www.forbes.com/sites/alisoncoleman/2014/10/01/germanys-security-start-ups-leading-a-global-demand-for-online-data-privacy/>.

132. GERMAN INSTITUTE FOR TRUST AND SECURITY ON THE INTERNET (DIVSI), *STUDY DATA – COMMODITY AND CURRENCY*, (Nov. 17, 2014), <https://www.divsi.de/publikationen/studien/divsi-studie-daten-ware-und-waehrung/zentrale-erkenntnisse/>; see also Erika Körner, *One-third of German internet users would pay for data protection. survey finds*, EUROACTIV (Nov. 18, 2014), <http://www.euractiv.com/sections/innovation-enterprise/one-third-german-internet-users-would-pay-data-protection-survey>.

133. Monica Horten, *Germany v. Britain Tussle Over New EU Data Privacy Rules*, IPTEGRIITY (Aug. 6, 2013), <http://www.iptegrity.com/index.php/european-union/privacy/899-germany-v-britain-tussle-over-new-eu-data-privacy-rules>.

134. Council Directive 95/46/EC, *supra* note 24, at art. 28.

135. See generally, Case C-614/10, *Comm'n v. Austria*, 2012 E.C.R. 631 (2012).

with complete independence.¹³⁶

Despite the Directive's ideal objective of establishing independent agencies that protect data in a consistent and uniform way, the reality is that these agencies are hardly independent. They are each staffed with government officials from their respective countries and are asked to regulate in accordance with each country's local data protection framework.¹³⁷ After all, there is a reason why Germany is seen as boasting the strictest data protection regulations and the UK maintains a reputation for being more industry-friendly. While many of these agencies do not appear as blatantly influenced by national governments as the Austrian agency was in 2012,¹³⁸ it strains credulity to suggest that they are completely independent entities. Consequently, the ECJ's holding delivers a significant blow to those data protection agencies who take a more light-handed approach in their regulation of data protection.

C. Preservationism vs. Deletism

As previously mentioned, *Google Spain* establishes an important precedent with respect to "the right to be forgotten." For the past decade or so, dozens of scholars have commented on and written at length about whether there truly exists a right to be forgotten, and if so, what its parameters are.¹³⁹ While it is not the purpose of this paper to delve deep into the merits and demerits of a right to be forgotten, any analysis of the ECJ's decision would be incomplete without at least addressing its impact on this heated debate.

In general, the controversy surrounding the right to be forgotten has become so contested that labels have been attributed to the competing sides. On one side of the debate stand the "Preservationists."¹⁴⁰ This cohort consists of those who believe that the people of today owe the entire internet to their descendants.¹⁴¹ Preservationists embrace the fact that more information about the everyday lives of people is being doc-

136. *Id.* ¶ 25.

137. Council Directive 95/46/EC, *supra* note 24, at art. 28(1)(2).

138. Case C-614/10, *supra* note 135, at 9.

139. Compare Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. 88 (2012) (asserting that the right to be forgotten addresses an urgent problem in the digital age), with Emily Adams Shoor, *Narrowing the Right to be Forgotten: Why the EU Needs to Amend the Proposed Data Protection Regulation*, 39 BROOK. J. INT'L L., 487, 489 (2014) (suggesting that the ambiguity of the right to be forgotten will have a chilling effect on freedom of expression that outweighs its personal privacy benefits).

140. Ambrose, *supra* note 105, at 396.

141. *Id.*

umented online.¹⁴² Researchers have up until now been forced to rely on whatever physical documents happened to survive the trials of time.¹⁴³ With the internet, however, historians can potentially have complete access to the vast digital legacies left behind by today's internet users.¹⁴⁴ In other words, what may look like irrelevant information to some would be seen as a valuable piece of history in the eyes of a preservationist.

On the other side of the debate are the "Deletionists."¹⁴⁵ This school of thought is comprised of those who believe that forgetting must be a part of the internet in order to promote efficient, useful, and high-quality information practices.¹⁴⁶ In his 2009 book, *Delete: The Virtue of Forgetting in the Digital Age*, self-proclaimed Deletionist Viktor Mayer-Schönberger argues that a comprehensive memory is as much a curse as it is a boon.¹⁴⁷ Too perfect a recall, he contends, prompts people to become caught up in their memories.¹⁴⁸ This inability to leave the past behind makes life more unforgiving in the digital age than ever before.¹⁴⁹ He cites the example of a psychotherapist who was trying to cross the U.S. – Canadian border in 2006.¹⁵⁰ The border patrol officer ran a quick search on the internet and found a 1960's academic paper where the man admitted he had taken LSD.¹⁵¹ This was enough cause to deny the man entry into the U.S.¹⁵² Putting the reasonableness of border policies aside, one's digital footprint, it appears, has become more of a specter than a keepsake.

Google Spain has resulted in a major victory for the Deletionists. Mr. González, like all other Deletionists, wanted to control the extent to which information about his life was being processed and disseminated

142. Sumit Paul-Choudhury, *Digital Legacy: The Fate of Your Online Soul*, NEW SCIENTIST (May 15, 2012), <http://www.newscientist.com/article/mg21028091.400-digital-legacy-the-fate-of-your-online-soul.html>.

143. *Id.*

144. *Id.*

145. Meg Leta Ambrose, *A Digital Dark Age and the Right to be Forgotten*, 17 No. 3 J. INTERNET L. 1 (2013).

146. *Id.*

147. See generally, VIKTOR MAYER-SCHONBERGER, *DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE* (2009); see also Stuart Jeffries, *Why We Must Remember to Delete – and Forget – in the Digital Age*, THE GUARDIAN (Jun. 30, 2011), <http://www.theguardian.com/technology/2011/jun/30/remember-delete-forget-digital-age>.

148. Jeffries, *supra* note 147.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

on the internet. By ordering Google to grant his removal request, the ECJ gave credence to the Deletionist philosophy. A preservationist would have approached this case in a completely different way. Instead of looking at things from the data subject's perspective, a preservationist would have adopted the perspective of internet users in general, including those in the future. Greater value would have also been attributed to Mr. González's social security debts as well. The ECJ casted that information aside like a derelict on the seas of the internet, whereas a preservationist would have deemed it an appreciable token of the past worthy of archiving. Nevertheless, the Deletionist school of thought has won the day. It now enjoys the backing of the ECJ as well the many others who call for an increase in the regulation of personal data online.

In 1937, H.G. Wells compiled a collection of essays and lectures into a book entitled *World Brain*.¹⁵³ Within this book, Wells envisioned a permanent world encyclopedia, an efficient index to all human knowledge, ideas, and achievements.¹⁵⁴ He was so unabashedly confident that a planetary memory for all mankind was on the horizon that he wrote the following:

This is no remote dream, no fantasy. It is a plain statement of a contemporary state of affairs. It is on the level of practicable fact. It is a matter of such manifest importance and desirability for science, for the practical needs of mankind, for general education and the like, that it is difficult not to believe that in quite the near future, this Permanent World Encyclopaedia, so compact in its material form and so gigantic in its scope and possible influence, will not come into existence.¹⁵⁵

Wells professed the idea that the world would be much better off if people had instantaneous access to everything that has ever been learned.¹⁵⁶ Better decisions would be made, better actions would be taken, and better lives would be led.¹⁵⁷ Whether or not his assertions hold water, one cannot dispute the prophetic nature of Wells' writing: Google is the World Brain.¹⁵⁸ "[T]he core" of Google is the creation of a "world synthesis of bibliography and documentation with the indexed archives of the world."¹⁵⁹ "A great number of [people] are engaged per-

153. H.G. WELLS, *WORLD BRAIN* (1938).

154. *Id.* at 60.

155. *Id.* at 61.

156. *See id.* at 60-61.

157. *See id.*

158. Jeffries, *supra* note 147.

159. WELLS, *supra* note 153, at 85.

petually in perfecting this index of human knowledge and keeping it up to date.”¹⁶⁰ This is the epitome of what preservationists praise and Deletionists detest. To use the words of Mayer-Schönberger, “[q]uite literally, Google knows more about us than we can remember ourselves.”¹⁶¹

In keeping with the Wellsian analogy, the ECJ’s holding in *Google Spain* acts like a toxin that kills some of the world’s brain cells. Each time an individual requests that their data be stricken from Google’s search results, a piece of information is ripped out of the permanent encyclopedia. Google and the internet in general have proven to be the most powerful informational tools since Gutenberg’s printing press. The ECJ’s decision has essentially given data subjects the ability to detract from this tool at the expense of all other users. According to the ECJ, the World Brain ought to work as the ECJ wants it to, operating under its terms and abiding by its rules. This commanding approach unfortunately harms the World Brain in such a way that a step is taken away from, rather than towards, a free and open society.

D. The Economic Repercussions of the ECJ’s Decision

As examined above, there are many ways in which *Google Spain* has done harm to the individuals and institutions of Europe. A disservice is imposed upon individual internet users, people looking to express themselves, internet search engine operators, and even the data protection agencies enforcing the ECJ’s decision. There is yet another major area of Europe that gets hit hard by *Google Spain*, an area which has not yet received sufficient attention. That area is the European market economy.

It is no secret that over the past decade the economic climate of the European Union has been quite dismal. Inflation rates went up, member states looked for bailouts, and confidence in central banks waned.¹⁶² Within the past several years, though, many positive signs of recovery have been reported.¹⁶³ The outcome of *Google Spain*, however, does anything but further the economic interests of a region that is looking to seize every opportunity it can to hasten its road to recovery.

160. *Id.*

161. Jeffries, *supra* note 147.

162. See generally Caroline Bradley, *From Global Financial Crisis to Sovereign Debt Crisis and Beyond: What Lies Ahead for the European Monetary Union?*, 22 *TRANSNAT’L L. & CONTEMP. PROBS.* 9, 12, 17 (2013).

163. Ross Finley, *For first time in years, euro economy starts surprising on upside*, *REUTERS* (Mar. 4, 2015, 7:25 AM), <http://www.reuters.com/article/2015/03/04/us-europe-economy-poll-analysis-idUSKBN0M019220150304>.

The ECJ's decision adversely impacts the European economy because it fails to appreciate the rapidly evolving marketplace, one that looks a lot different today than it did twenty years ago when Directive 95/46 was enacted. To illustrate this stark difference, consider the major role that personal data plays in the modern economy. As the internet continues to blossom into a universal informational tool, personal data has become monetized into a very valuable form of currency. Companies use this information to improve their business models and maximize their ability to provide people with goods and services. For example, many companies rely on Google's search engine services to conduct research. The poor search visibility encouraged by the ECJ imposes a high transactional cost on these companies because finding information is no longer uncovered by a simple search.¹⁶⁴ This increased cost of business will eventually be paid for by consumers, usually in the form of higher prices. In other words, because the ECJ's decision now limits the amount of information companies can access, both producers and consumers must suffer.

Those who do not believe that higher levels of data protection hinder economic progress are likely to point to Germany, a nation with strict data protection laws that is touted as having the strongest economy in Europe.¹⁶⁵ A recent leak in government documents, however, brings into question Germany's true stance on data protection. In March of 2015, thousands of classified documents revealed the efforts of many European governments to weaken a new data protection framework that will replace Directive 95/46.¹⁶⁶ Despite its public statements in support of more data protection, the leaked documents show Germany is now leading the pack among member states seeking more business-friendly standards.¹⁶⁷ Moreover, Germany's data protection agency has a reputation for being aggressive in announcing its investigations of non-compliance, but is much more reluctant in actually using its powers.¹⁶⁸ Perhaps this is because Germany realizes that its economic interests are better served by opening up its markets to the internet rather than in-

164. Selinger & Hartzog, *supra* note 109.

165. Richard Anderson, *German economic strength: The secrets of success*, BBC NEWS, (Aug. 16, 2012), <http://www.bbc.com/news/business-18868704>.

166. Nikolaj Nielsen, *German-led moves to weaken EU data bill a 'scandal,'* EU OBSERVER (Mar. 11, 2015, 18:21 PM), <https://euobserver.com/justice/127961>.

167. *Id.*

168. Marc Dautlich et al., *Data protection enforcement in UK, France and Germany explained*, OUT-LAW.COM (Jul. 5, 2013), <http://www.out-law.com/en/articles/2013/july/data-protection-enforcement-in-uk-france-and-germany-explained/>.

creasing its data protection measures. Instead of refuting the economic impediments of data protection, pointing to Germany might actually be a way of establishing that those impediments actually do exist.

V. CONCLUSION

The European Court of Justice made a number of crucial mistakes in *Google Spain*. It appears that these mistakes stem from the Court's primary concern for an individual's right to privacy and data protection. While this concern is undoubtedly admirable, it unfortunately tramples on other fundamental rights such as the freedom of expression. Moreover, it excessively impinges on the public's interest in accessing information and the benefits to be obtained therefrom. These considerations deserve ample attention as the European Union continues to piece together its data privacy laws in the forthcoming General Data Protection Regulation. Ultimately, the court's blind eye has led it to serve an injustice to the people of Europe.