Google LLC v. Commission Nationale de L'informatique et des Libertés (CNIL): Does Everyone Have to Listen to the European Union?

I. OVERVIEW

The Commission Nationale de L'Informatique et des Libertés (French Data Protection Authority, France) (CNIL), which is the national French data protection agency, notified Google LLC (Google) that when the search engine grants an individual's request to remove links populated from a search of the person's name, it must remove those links on all of its domain name extensions.[1] Google refused, limiting its removal of links at issue to Member States in the European Union (EU).[2] After the deadline to comply with the notice passed, Google offered to implement a geo-blocking technique where the search engine would use an Internet user's IP (Internet Protocol) address to limit the user's access to the links at issue.[3] The CNIL found the geo-blocking proposal to be insufficient[4] and fined Google 100,000 euros for the search engine's refusal to de-reference an individual's online profile on all of the search engine's domain name extensions.[5] Google, successor in law to Google Inc., sued the CNIL in the Conseil d'État to annul the CNIL's findings.[6] The Conseil d'État (Council of State, France) found that Google is subjected to French law.[7] Google

1. The President of the CNIL served the notice on May 21, 2015. Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), 2019 EUR-Lex CELEX No. 62017CJ0507 (Sept. 24, 2019), ¶ 30. *See generally id.* ¶ 36 (explaining how search results may be different on several domain names such as google.fr or google.de).

2. *Id.* ¶ 31.

3. *Id.*

4. *Id.* ¶ 32.

5. The CNIL made this finding on March 10, 2016. *Id.* ¶ 33.

6. *Id.* ¶ 2.

7. Google France operates on French territory, so Google is subjected to the French Law of 6 January 1978. *Id.* ¶ 37.

contended that the CNIL misinterpreted the law because, while the EU recognizes the right to de-referencing, the jurisdictional reach concerning that right does not mandate the erasure of links on all of its search engine's domain names.[8]

The Conseil d'État referred the issue of the territorial scope of the right to de-referencing to the Court of Justice of the European Union (EJC) for a preliminary ruling.[9] The EJC was tasked with determining whether a search engine must remove links on a national level, on a Union level, or on a worldwide level.[10] Additionally, the Court had to determine whether the search engine must employ a geo-blocking technique to carry out the removal of the links at issue.[11] The EJC *held* that a search engine operator is required to de-reference only on versions of that search engine corresponding to all the Member States, using measures, such as geo-blocking technology, to effectively prevent or seriously discourage an Internet user from accessing the removed links. Case C-507/17, *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, 2019 EUR-Lex CELEX No. 62017CJ0507 (Sept. 24, 2019).

II. BACKGROUND

A. Legal Context

Treaties among European countries hold privacy rights, specifically data protection, to a high level of protection.[12] Article 16 of the Treaty on the Functioning of the European Union (TFEU)[13] and articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter)[14] provide the legal basis for the protection of personal data as a fundamental

8. *Id.* ¶ 38.
9. *Id.* ¶ 39.
10. *Id.*
11. *Id.*
12. *See generally* Udo Bux, *Personal Data Protection*, EUR. PARLIAMENT (May 2019), http://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection (providing the legal history of personal data protection in the European Union).
13. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 55 [hereinafter TFEU] ("Everyone has the right to the protection of personal data concerning them.").
14. Charter of Fundamental Rights of the European Union art. 7, Oct. 26, 2012, 2012 O.J. (C 326) 391 [hereinafter Charter] (stating that everyone has the right to respect their private and family life, home, and communication); *see also id.* art. 8 ("Everyone has the right to the protection of personal data concerning them."). *See generally* Charter of Fundamental Rights, EUR-LEX, https://eur-lex.europa.eu/summary/glossary/charter_fundamental_rights.html (last visited Nov. 18, 2019) (providing that the Charter of Fundamental Rights is binding and consolidates EU-level fundamental rights).

right. The right to privacy and the protection of personal data are closely related fundamental rights but are nonetheless distinct.[15] The European Convention on Human Rights provides for a right to respect for private and family life (article 8) and freedom of expression (article 10).[16] The laws created to provide for or protect the rights and freedoms the Charter sets out are subjected to the principle of proportionality: "limitations may be made only if they are necessary and genuinely meet objectives of general interest recogni[z]ed by the Union or the need to protect the rights and freedoms of others."[17] The legislations are primarily limited to the EU's borders.[18]

Regulation 2016/67 (General Data Protection Regulation) (GDPR) is the current EU legislative on data protection.[19] Article 16 of the TFEU and articles 7 and 8 of the Charter are the legal basis for the GDPR.[20] This law repealed Directive 95/46/EC, the EU's former legal framework on data protection.[21] The EU Parliament adopted the GDPR in 2016 and the GDPR became enforceable throughout the twenty-eight-country bloc in 2018.[22] The GDPR provides for the protection of personal data for individuals in an increasingly data-driven world.[23] Because this legal framework was implemented into the regulations of the EU, the rules ensure that the high level of protection of people's rights and freedoms are applied consistently.[24] Additionally, the GDPR provide a clearer framework for data-collection or related business under EU jurisdiction.[25]

The GDPR provides for the rights of the data subject and the responsibility of the processor of the individual's data.[26] The data subject must give affirmative consent to the data process and receive information

---

15. European Data Prot. Supervisor, *Data Protection*, EUR. UNION, https://edps.europa.eu/data-protection/data-protection_en (last visited Nov. 18, 2019).

16. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, arts. 8, 10, 213 U.N.T.S 221 [hereinafter European Convention on Human Rights]; *see also id.* at art. 10 (further providing that certain information may be prevented from being disclosed).

17. *See* Charter, *supra* note 14, art. 52.

18. *See id.*; TFEU, *supra* note 13, art. 355.

19. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR], 2019 O.J. (L 119) 1; *see also* European Data Protection Supervisor, *supra* note 15.

20. *See generally* Bux, *supra* note 12.

21. GDPR, *supra* note 19, art. 94.

22. European Data Prot. Supervisor, *supra* note 15.

23. GDPR, *supra* note 19, recitals 9, 10.

24. *Id.* recital 10.

25. *Id.* recital 5.

26. *Id.* art. 6.

and notice of the data-processing from the controller.[27] Among the recognition of many rights pertaining to privacy in an electronic age, Article 17 of the GDPR codified the right to erasure ("right to be forgotten").[28] The right to erasure allows citizens to ask for their data to be deleted where "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed."[29] The right to erasure does not apply to processing of data that exercised the right of freedom of expression and information or necessary to protect public interest.[30] Singling out an individual for a protected characteristic is prohibited via data processing.[31]

Article 9 does provide exceptions to article 17.[32] A data subject may consent to the data processing of personal information.[33] Processing of personal data is necessary in certain situations in the fields of employment, health, or social security or in a legal capacity.[34] Data may be processed to protect the vital interest of the individual or the public.[35] Processing of personal data is permitted if carried out in the course of legitimate activities.[36] These exceptions are assessed based on the principle of necessity and proportionality.[37]

Just like the treaties that provide for the GDPR legal basis, the right to be forgotten is subject to the principle of proportionality.[38] While the GDPR acknowledges that the protection of personal data is a fundamental right, it is not an absolute right.[39] The fundamental right must be balanced against other fundamental rights, such as freedom of expression and information,[40] and "must be considered in relation to its function in society."[41] A data subject has the right to be forgotten where the data

27. *Id.* art. 7.
28. *Id.* art. 17.
29. *Id.*
30. *Id.* art. 18.
31. *Id.* art. 9 ("[R]evealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.").
32. *Id.*
33. *Id.*
34. For example, a physician needs a patient's medical history to aptly treat the individual, which may transmit the data electronically, and article 9 provides that processing is allowed. *Id.*
35. *Id.*
36. *Id.*
37. *See id.* recital 154; art. 35(7).
38. *Id.* recitals 4, 150; art. 35(7).
39. *Id.* recital 4.
40. *Id.*; *see also id.* art. 85.
41. *Id.* recital 4.

processing violates the laws of the EU or the laws of a Member State, except where the retention of the personal data is necessary or lawful.[42]

A controller not complying with the GDPR may be issued a warning or a fine.[43] A controller is a person or entity that "determines the purposes and means of the processing of personal data" by automated means or other means of filing.[44] The territorial scope applies to businesses with an establishment in the EU, regardless of where the data processing occurred.[45] Even without an establishment in the EU, the GDPR applies where the processing activities relate to the offering of goods or services or where the data subjects are monitored by the processing activities.[46] The GDPR applies to organizations without an establishment in the EU by virtue of public international law.[47]

With the historic implementation of the GDPR in 2016, the EU's legislation ensured privacy rights to citizens of Member States, impacted international operating entities, and influenced third-party countries to consider the ratification of data protection as a fundamental right.[48] For example, companies like Facebook and Uber, in complying with the GDPR, updated their service agreements not only for users based in the EU, but for users worldwide.[49] Countries such as Brazil, Japan, and South Korea have introduced bills or passed legislations for privacy rights similar to the GDPR.[50]

The 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 ("Data Protection Directive"), succeeded and repealed by GDPR, provided the previous protective measures for personal data.[51] The Data

---

42. *Id.* recital 65.
43. *Id.* arts. 58, 83.
44. *Id.* arts. 2, 4.
45. *Id.* art. 3.
46. *Id.*
47. *Id.*
48. Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html?module=inline.
49. See *id.*; *see also* FACEBOOK for Bus., *What Is the General Data Protection Regulation (GDPR)?*, FACEBOOK, https://www.facebook.com/business/gdpr (last visited Nov. 19, 2019).
50. Satariano, *supra* note 48.
51. GDPR, *supra* note 19, art. 94; *see also* 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) 1, 31 [hereinafter Data Protection Directive].

Protection Directive, adopted in 1995 when the Internet was relatively new, drew its legal basis on articles 8 and 10 of the European Convention on Human Rights.[52] The Directive aimed to protect the fundamental right to privacy with respect to the processing of personal data.[53] Article 12(b) states that a data subject may demand "erasure or blocking of data processing" in violation of the Directive, "in particular because of the incomplete or inaccurate nature of the data."[54]

Individuals must have "compelling legitimate grounds" to request the controller of the data processing to remove their personal information pursuant to article 14 of the Directive.[55] Under the Directive, a controller is anything or anyone that "determines the purposes and means of the processing of personal data."[56] Processing of personal data is "any operation . . . which is performed upon personal data, whether or not by automatic means."[57] The Directive balances fundamental rights to privacy, freedom of expression, and the legitimacy of the data processing in providing for the erasure of the data or an exemption to the Directive.[58] The fundamental rights of individuals with freedom of information, in particular the right to receive and impart information,[59] stipulates an exemption for journalism or literary or artistic expression.[60]

To ensure a high level of protection of personal data throughout the EU, Member States adopted a national provision in accordance to the Directive.[61] The jurisdiction extended over establishments in the EU that carried out the processing regardless of whether or not the processing took place in the EU.[62] Even if the controller was located in a third-party country outside the EU, the Directive may apply by virtue of international

52. Data Protection Directive, *supra* note 51, ¶¶ 10, 37.
53. *Id.* art. 1.
54. *Id.* art. 12(b).
55. *Id.* art. 14.
56. *Id.* art. 2(d). The definition of controller as defined in the GDPR follows closely to the definition of controller in the Data Protection Directive. *See* GDPR, *supra* note 19, art. 4(7); Data Protection Directive, *supra* note 51, art. 2(d).
57. *Id.* art. 2(b) (listing means such "as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction").
58. *Id.* recital 37.
59. European Convention of Human Rights, *supra* note 16, art. 10.
60. Data Protection Directive, *supra* note 51, recital 37.
61. *See id.* art. 4.
62. *Id.*

public law.[63] Falling within the jurisdiction of the Directive, sanctions may be imposed on a controller, but a controller may also appeal such actions.[64]

After the EU passed the Directive in 1995, France implemented the Directive into its law by amending the Law No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (Law of 6 January 1978) with the passing of the Directive 2004-802 6 August 2004 (2004 Law).[65] The Law of 6 January 1978 states that technology should "not violate human rights, privacy, or individual or public liberties."[66] In particular, this law applies to data processing.[67] The CNIL was created to deal with and ensure the protection of data processing.[68] A controller of the data processing may be fined if it violates the law.[69]

B. Establishing the Right to De-Referencing

The EJC is responsible for interpreting EU law and ensuring the law is applied uniformly in all of the EU Member States.[70] National courts of the Member States have to follow EU law, but when the issues of interpretation or validity of an EU law are in question, the courts may petition the EJC for clarity on the law.[71] In 2014, an interpretation issue arose from the Data Protection Directive from which the EJC recognized the right to de-referencing in *Google Spain v. Google*.[72]

The recognition in *Google Spain* was based on article 12(b) and subparagraph (a) of the first paragraph of article 14 of the Data Protection Directive.[73] The EJC held that the individual has a fundamental right to

---

63. *Id.*

64. *Id.* art. 24.

65. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (version consolidée au 27 août 2011) [Law 78-17 of January 6, 1978, on Information Technologies, Data Files and Civil Liberties (consolidated version as of Aug. 27, 2011)], LEGIFRANCE, http://legifrance.gouv.fr/affichTexte.do;jsessionid=46284B7113DCD877F7481BE7C32348A2.tpdjo10v_1?cidTexte=JORFTEXT000000441676&categorieLien=id, *translation at* https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf (lasted visited Jan. 14, 2020).

66. *Id.* art. 1.

67. *Id.* art. 2.

68. *See id.* arts. 11, 45.

69. *Id.* art. 45.

70. *See* ANTHONY ARNULL, THE EUROPEAN COURT OF JUSTICE 627 (2d ed. 2006) ("The general position is and always has been that the Court of Justice is not bound by its previous decisions but that in practice it does not often depart from them."); *see also Court of Justice of the European Union (CJEU)*, EUR. UNION, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last visited Nov. 14, 2019).

71. *Id.*

72. Case C-131/12, Google Spain v. Google, 2019 EUR-Lex CELEX No. 62012CJ0131 (May 13, 2014), ¶ 88.

73. *Id.* ¶ 100(3-4).

remove links relating to his name from a search engine's list of results.[74] De-referencing requires search engines to remove links that pertain to an individual based on a search of the individual's name.[75] The EJC reasoned that such a request will be balanced against the interests of the general public, the individual's fundamental rights, and the economic interest of the search engines; the fundamental legal basis of the right is subjected to the principle of proportionality.[76] The EJC also held that a search engine operator who established a branch or subsidiary in a Member State for the purpose of promoting and selling advertising space towards the inhabitants of that Member State is within the jurisdiction of the EU and subjected to the Data Protection Directive.[77]

III. COURT'S DECISION

In the noted case, the EJC determined the territorial scope of the right to de-referencing by considering the GDPR, the current data protection framework, and the Data Protection Directive, an earlier framework.[78] Although the GDPR repealed the Directive, Google sued the CNIL under French law, which implemented the Directive into law as the Law of 6 January 1978, and thus the Directive is applicable in the noted case.[79] First, the EJC analyzed the legal basis of its judgment in *Google Spain* and article 17(1) of the GDPR to determine the extent of the right to de-referencing.[80] Second, having examined the legal basis and development in legal authority to secure and enforce the right to de-referencing, the Court found that the right is applicable at the EU level.[81] Lastly, the Court reasoned that search engine operators are required to take measures to ensure the protection of that right.[82]

First, the EJC looked at the pertinent law: Article 12(b) of the Data Protection Directive, which deals with the right of access, in particular, erasure or blocking of incomplete or inaccurate data that have been processed;[83] subparagraph (a) of the first paragraph of article 14 grants the

74. *Id.* ¶ 100(4).
75. *Id.*
76. *Id.* ¶ 99.
77. The EJC interpreted article 4(1)(a) of the Data Protection Directive. *Id.* ¶ 2.
78. Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), 2019 EUR-Lex CELEX No. 62017CJ0507 (Sept. 24, 2019), ¶ 41.
79. *Id.*
80. *Id.* ¶ 43.
81. *Id.* ¶ 74.
82. *Id.*
83. Data Protection Directive, *supra* note 51, art. 12(b).

data subject's right to object based on compelling legitimate grounds of the Data Protection Directive;[84] and article 17(1) of the GDPR provides the right to erasure or the right to be forgotten.[85] The Directive and GDPR guarantee a high level of protection of personal data throughout the EU.[86] The Court emphasized that while data protection is a fundamental right, it is not an absolute right.[87] Subjected to the principle of proportionality, article 17 of the GDPR found a balance between the individual's rights,[88] such as privacy and protection of personal data, with the freedom of information of Internet users at the EU-level.[89] Although de-referencing worldwide would accomplish the objective, many countries outside the EU have not recognized the right to de-referencing or they have different ways of addressing that right.[90]

Second, the Court considered the intention of the EU, ultimately deciding that de-referencing is at the EU-level.[91] By elevating the legal status of data protection from a directive to a regulation for the purposes of ensuring a consistent and high level of protection throughout the EU bloc, the EU legislature did not intend for de-referencing to be limited to just where the request was made but for it to extend to all of the Member States.[92] Since the Regulation and Directive explicitly provide for the right to de-referencing within the EU and no EU law provides for that right beyond its borders, the search engine is required to carry out de-referencing "on the versions of that search engine corresponding to all the Member States."[93] The Court briefly noted that the laws of the EU do not prohibit the practice of de-referencing on all versions of the search engine.[94]

Third, the Court discussed that the search engine operator must take effective measures to protect an individual's personal data.[95] The measures must meet legal requirements and prevent or at least discourage users in the Member States from accessing the removed links.[96] Google

84. *Id.* art. 14.
85. GDPR, *supra* note 19, art. 17.
86. Case C-507/17, *Google*, 2019 EUR-Lex CELEX No. 62017CJ0507, ¶ 54.
87. *Id.* ¶ 60.
88. *Id.* ¶¶ 61-63.
89. *Id.* ¶¶ 60-61.
90. *Id.* ¶¶ 55, 59.
91. *Id.* ¶ 66.
92. *Id.* ¶¶ 64, 66.
93. *Id.* ¶ 74.
94. *Id.* ¶¶ 64, 72.
95. *Id.* ¶ 70.
96. *Id.*

implemented a new process where an Internet user is automatically directed to the national version of the search engine that corresponds to the place of the presumed search and results displayed are determined by a geo-location process during consideration before the court.[97] Because of this new geo-processing measure, the EJC will allow the referring court, the Conseil d'État, to determine whether Google's geo-blocking complies with the requirement set out in its judgment.[98]

IV. ANALYSIS

While the EJC focused on the principle of proportionality in determining the territorial scope of the right to de-referencing, the decision left open the possibility of a broader interpretation and potential effect of the EU imposing its beliefs on third-party countries or entities.[99] The EU is leading the charge on privacy rights to ensure that individuals maintain their privacy in the ever-growing Internet age.[100] The right to de-referencing is a recognized fundamental right in the EU, but that right is not recognized everywhere in the world.[101] There is a difference between leading the charge and forcing autonomous groups to follow along.[102] That line is sometimes obfuscated by a championship of a fundamental right and the cultural or economic direction of another country.[103]

This case is important because it establishes the territorial scope of the right to de-referencing, extending to the borders of EU Member States.[104] While clarifying the jurisdictional boundary, the EJC emphasized the proportionality principle by considering the rights of the individual and the right of the public.[105] The Court recognized that, among differing global temperaments, the Member States may also embrace and regulate de-referencing differently.[106] A positive implication is that, having been explicitly provided for in the EU's regulation, the right to de-referencing is read broadly to protect the individual from the emergence of data-collection from countries or big corporations, without

97. *Id.* ¶ 42.
98. *Id.* ¶ 71.
99. *Id.* ¶¶ 64, 72.
100. European Data Protection Supervisor, *supra* note 15.
101. Case C-507/17, *Google*, 2019 EUR-Lex CELEX No. 62017CJ0507, ¶ 60.
102. Satariano, *supra* note 48.
103. Adam Satariano, *Europe Is Reining in Tech Giants. But Some Say It's Going Too Far*., N.Y. TIMES (May 6, 2019) https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html?module=inline.
104. Case C-507/17, *Google*, 2019 EUR-Lex CELEX No. 62017CJ0507, ¶ 66.
105. *Id.* ¶¶ 60, 63.
106. *Id.* ¶ 67.

overreaching the EU's jurisdiction.[107] In delivering a decision that curtailed the jurisdictional reach, the EJC acknowledged that the law does not eliminate the possibility that the circumstances call for a broader, and potentially worldwide, application.[108]

The EU's Internet privacy laws deal with personal information that is considered old, no longer relevant, or no longer in the public's interest to have the information published in the Internet.[109] This lends to the idea of removing information that is no longer relevant and may stigmatize people.[110] However, the interpretation may be taken too far, as in the case of a man who stabbed his brother many years ago and won his challenge to remove an article about the attack, as he contended that this history prejudiced him from his community.[111] The journalist who reported that story had to remove the web links featuring the attack.[112] The implication that arises is that the right to de-referencing could be used to suppress speech.[113] Suppression of speech by offended political figures is always a concern because it would be an avenue to unjust censorship.[114] Other countries may invert the intention of the EU's protection of the individual into unjust censorship, such as banning or erasing political dissent.[115]

The EJC could have been influenced by Europe's societal context and its heightened sensitivity to privacy.[116] The EU, through treaties and legislative instruments, has displayed a high interest in protecting individuals' personal data.[117] The EU's challenge to the rest of the world to follow in its lead is aspirational.[118] However, to demand autonomous countries to bend to the will of another country may invite unintended consequences.[119]

---

107. *See id.* ¶ 74.

108. *Id.* ¶¶ 64, 72.

109. *See* GDPR, *supra* note 19, art. 5(1)(d); *see also* Adam Satariano & Emma Bubola, *One Brother Stabbed the Other. The Journalist Who Wrote About It Paid a Price.*, N.Y. TIMES (Sept. 23, 2019), https://www.nytimes.com/2019/09/23/technology/right-to-be-forgotten-law-europe.html?action=click&module=RelatedLinks&pgtype=Article.

110. Satariano & Bubola, *supra* note 109.

111. *Id.*

112. It was too costly for the journalist to keep contesting individuals' requests to remove stories purporting factual events, so the journalist no longer operates the news website. *Id.*

113. *Europe Is Reining in Tech Giants. But Some Say It's Going Too Far*, *supra* note 103.

114. *See id.*

115. *See id.*

116. Satariano, *supra* note 48.

117. Bux, *supra* note 12.

118. *See* Satariano, *supra* note 48.

119. *Id.*

V. CONCLUSION

Google does not have to remove links on a worldwide scale, but the EJC's judgment favoring Google in regard to information, privacy, and speech protection may be a Trojan Horse as the Court does not foreclose the possibility of a worldwide directive. In considering the territorial reach, the Court weighed the right to de-referencing against other rights along with the existence of different views on de-referencing within the EU and outside of the EU.

The right to de-referencing extends to the borders of the EU, so the search engine must remove links on all of its versions within the EU. As the EU is leading the charge on privacy protection, even with the territorial limitation of the right, a future ruling may overreach and weaken the Court's jurisdiction and the EU's authority. No single entity should possess the authority to regulate access to information over another autonomous entity.

Tu Huynh*

 J.D. candidate 2020, Tulane University Law School; B.A. 2017, Louisiana State University. The author would like to thank her parents and the members of the *Tulane Journal of International and Comparative Law* for their guidance and advice throughout this process.