Implications of the Right To Be Forgotten

Aidan Forde*

I. INTRODUCTION: THEORETICAL DISCUSSION UNDERLYING THE RIGHT TO BE FORGOTTEN

In a world where search engine results can define individual identity, information that lingers in the online sphere can sometimes have overwhelmingly negative consequences. In modern society, focus is placed on remembering rather than forgetting; "[t]oday, forgetting has become costly and difficult, while remembering is inexpensive and

* © 2015 Aidan Forde. BCL (Int) LL.M. (Cantab), aidan.forde@cantab.net. The author thanks Dr. Kirsty Hughes of Clare College, University of Cambridge, for her guidance in the completion of this Article.

easy."[1] Warren and Brandeis's 1890 seminal "right to be let alone" piece encouraged the individual "to decide whether that which is his shall be given to the public."[2] The authors could not have anticipated the impact that technology would have on privacy rights, but did declare that such rights applied to "any modern device" that could affect privacy.[3] This permits individuals to control and organize their private life as they see fit.[4] The creation of a right to be forgotten derives from privacy harms the online world has created. The unforgiving nature of online content makes it difficult for the individual to choose which information about him is accessible or suppressed. Content posted online becomes a "tattoo etched into ourselves, which is hard and cumbersome to remove."[5] Alterations to the existing legal framework are inevitable. This work asserts that the right to be forgotten ("the right") is a necessary development that should be embraced. Its creation will lead to positive implications for the individual's right to informational self-determination and overall judicial thinking.

Discussion of the right emerged in Mayer-Schönberg's book *Delete: The Virtue of Forgetting in the Digital Age*.[6] The author correctly identified that one of the main problems with data storage is an absence of the human characteristic to forget.[7] Van Hoboken noted how the concept has its foundation in legal qualifications such as the right to have information deleted, social forgetfulness, and the right to oblivion.[8] Koops questions whether it is in fact a right.[9] It can also be classified as an ethical and social value or a policy aim.[10] Rouvroy specifically

---

1. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 62-93 (2009).

2. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 199 (1890).

3. GEIR M. KOIEN & VLADIMIR A. OLESHCHUK, ASPECTS OF PERSONAL PRIVACY IN COMMUNICATIONS—PROBLEMS TECHNOLOGY AND SOLUTIONS 4 (2013).

4. Andra Giurgiu, *Challenges of Regulating a Right To Be Forgotten with Particular Reference to Facebook*, 7 MASARYK UNIV. J.L. & TECH. 361, 362 (2013).

5. Norberto Nuno Gomes de Andrade, *Oblivion: The Right To Be Different from Oneself: Reproposing the Right To Be Forgotten*, *in* THE ETHICS OF MEMORY IN A DIGITAL AGE: INTERROGATING THE RIGHT TO BE FORGOTTEN 65 (Hessla Ghezzi et al. eds., 2014).

6. MAYER-SCHÖNBERGER, *supra* note 1.

7. Ignacio Cofone, Google v. Spain*: A Right To Be Forgotten?*, 15 CHI.-KENT J. INT'L & COMP. L. 1 (2015).

8. Joris Van Hoboken, *The Proposed Right To Be Forgotten Seen from the Perspective of Our Right To Remember: Freedom of Expression Safeguards in a Converging Information Environment*, N.Y.U. L. INST. (May 2013), http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf.

9. Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice*, 8 SCRIPTED 3, 229-56 (2011).

10. *Id.*

formulates it as "a 'right' or rather a 'legitimate interest to forget and to be forgotten.'"[11] It could be a value or interest that requires protection or "a policy goal to be achieved by some means or other, whether through law or through other regulatory mechanisms."[12] There is not only the effect of being forgotten but also forgetting.[13] Both the right to be forgotten and enabling the individual to forget can be placed under an umbrella of oblivion, referred to in French as "droit à l'oubli" and "Diritto all'oblio" in Italian.[14] There is, however, a lack of consensus in defining the right with terms such as deletion, delisting/de-indexing, erasure, objection, and oblivion.[15]

A. The Rights Emergence

The emergence of a European right to be forgotten has its roots in the French right to oblivion.[16] This involves a convicted criminal having the opportunity to object to the publication of matters relating to their crime once the sentence has been served.[17] A criminal justice system that values societal reintegration may give the opportunity to prevent past-ills defining future existence. The French government was the first to conceive of the right, requiring online and mobile phone providers to eradicate text and e-mail messages after a certain period.[18] If rehabilitation has occurred, then an offender should have the opportunity to not have their previous offense haunt them.[19] The United Kingdom Rehabilitation of Offenders Act 1974 (UKROA) enables certain offenses to be ignored after a certain period.[20] The right would offer deletion of information that is no longer considered relevant in terms of newsworthiness.[21] Ambrose and Ausloos note that the underlying rationale is to protect the autonomy, personality, identity, and reputation

---

11. Antoinette Rouvroy, *Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?*, *in* THE SELECTED WORKS OF ANTOINETTE ROUVROY 249-78 (2008).

12. Koops, *supra* note 9, at 231.

13. *Id.*

14. Meg Leta Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right To Be Forgotten*, 16 STAN. TECH. L. REV. 369, 373 (2013).

15. Aurelia Tamò & Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 J. INTELL. PROP., INFO. TECH. & ELEC. COM. L. 1, 2 (2014).

16. Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

17. *See id.*

18. Rolf H. Weber, *The Right To Be Forgotten: More Than a Pandora's Box?*, 2 J. INTELL. PROP., INFO. TECH. & ELEC. COM. 120 (2011).

19. Robert Kirk Walker, *The Right To Be Forgotten*, 64 HASTINGS L.J. 257, 271 (2012).

20. *Id.*

21. *Id.*

of the individual.[22] In civilian jurisdictions it is common for certain criminal records to be removed or expunged after sentence has been served.[23] This primarily comes into consideration when the media make reference to past convictions. As Lindsay notes, civil law countries traditionally engage in a fact-specific balancing exercise between the "personality rights of the convicted" on one hand, and public interest/ freedom of expression parameters on the other.[24] Such personality rights involve values such as the right to private life, dignity, and honour.[25] These personality rights give the individual the autonomy to decide as to the possible use of data or information concerning them.[26]

The right is of particular relevance where an individual has served his sentence and desires the opportunity to suppress the publication of information about his conviction. The Swiss courts have used oblivion to deal with situations where the convicted individual wants to prevent their criminal records from gaining public attention.[27] Certain offenses may not require indefinite remembrance in the public sphere.[28] Where a "substantial amount of time" has passed since the offense, the public interest detaches.[29]

B. Terminology

As distinct from oblivion, a right of erasure gives the individual the option to demand removal of personal data that is held by third parties.[30] This aims to create a balance between data subjects and processors, handing more control to the right holder of the information.[31] Tamõ and George note that while oblivion is more concentrated on fundamental privacy protection and balancing contradictory interests, erasure involves enforcing a substantial claim.[32] A substantial claim involves a situation where treatment of personal information violates data protection

---

22. Meg Leta Ambrose & Jef Ausloos, *The Right To Be Forgotten Across the Pond*, 3 J. INFO. POL'Y 1, 14 (2013).

23. David Lindsay, *The "Right To Be Forgotten" in European Data Protection Law*, *in* EMERGING CHALLENGES IN PRIVACY LAW: COMPARATIVE PERSPECTIVES 302 (2014).

24. *Id.* at 303.

25. Weber, *supra* note 18, at 2.

26. *Id.*

27. *Id.*

28. *Id.*

29. Bundesgericht [BGer] [Federal Supreme Court] v. W., July 29, 1996, 122 ENTSCHEIDUNGEN DES SCHWEIZERISCHEN V. BUNDESGERICHTS [BGB] III 448 (Switz.).

30. Tamõ & George, *supra* note 15, at 73.

31. *Id.*

32. *Id.*

principles.[33] Legal tools of erasure help to empower data subjects.[34] This places checks on the use of personal data and controlling data over time. Article 12(b) of Directive 95/46/EC is enforced against the controller who "does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data."[35] This requires the controller to rectify information that is no longer accurate.[36] Article 14(a) enables the data subject to object "at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[37] Article 14(a) is the mechanism through which the individual can delete information related to him online.[38]

Three conceptions of the right are outlined by Koops.[39] First, the deletion of data in due time; second, a clean slate perspective;[40] and third, there exists a clean slate perspective that enables citizens to be able to express themselves without restraint.[41] Koops notes that this "aims at preventing people from suffering unduly from information about their past, with connections to the right to privacy and identity construction."[42] The option to have information deleted in due time involves placing an expiration date on content where the hindrances of retention start to overcome relative advantage.[43] This viewpoint is consistent with the right of erasure. As Xanthoulis observes, this conception assists in restricting third parties accessing personal information.[44] The "clean slate" perspective involves removing information that has been obtained in relation to an individual's past that is no longer relevant to their present and future.[45] The third conception falls within the psychological and social umbrella of privacy.[46] Koops references the need to ensure individual self-development and autonomy. An example is cookie

---

33. *Id.*
34. *Id.*
35. 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, art. 12(b), 2000 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].
36. *Id.*
37. *Id.* art. 14.
38. *Id.* art. 14(a).
39. Koops, *supra* note 9.
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.*
44. Napoleon Xanthoulis, *The Right to Oblivion in the Information Age: A Human-Rights Based Approach*, 10 US-CHINA L. REV. 84, 97 (2013).
45. *Id.* at 96.
46. *Id.* at 97.

retention by a social network or search engine, leading the individual to feel under surveillance.[47] Encompassing these three elements, it is Xanthoulis' correct assertion that a right of oblivion can be regarded as a "multidimensional right to privacy" amounting to a human right.[48]

C. Underpinning Normative Arguments

Autonomy runs at the core of the right. The creation of the right gives the individual increased control over information. A second understanding is viewing the right as a behavioural response to modern concerns. Social media has radically altered behaviour. Warren and Brandeis noted, "Political, social and economic changes entail the recognition of new rights . . . ."[49] With fundamental changes in the way individuals have their information processed, a reconceptualization of privacy is required. A right to be forgotten is a necessary development in this changing landscape.

An evolutionary understanding of the right gives regard to the benefits of forgetting. Lasica observed in 1998, "Everything you've ever posted online could come back to haunt you someday."[50] When data is lost, this is considered to be a failure from an information and communications technology (ICT) perspective.[51] This contrasts with the human desire to forget. Forgetting is a central element of human memory.[52] The very notion of forgetting a negative experience could be said to be part of trying to achieve greater success. Nietzche viewed forgetting as a "positive filter" to live a better life.[53] The brain places low priority on memories that are not needed in the future.[54] In contrast, the Internet does not categorize information as secondary or irrelevant. It operates as a constant collector of data that may one day be utilized. Time is essentially illusory online.

---

47. *Id.*

48. *Id.* at 98.

49. Warren & Brandeis, *supra* note 2, at 193; *see* Emma Fitzsimons, *Behind Closed Doors? Justifying What's Off Limits Online*, ELSA STUDENT J. EUR. L. 1, 11 (2014), https://sjeldraft.files.wordpress.com/2014/03/behind-closed-doors_-justifying-what_s-off-limits-online.pdf.

50. Angela Guimarães Pereira, Lucia Vesnić-Alujević & Alessia Ghezzi, *The Ethics of Forgetting and Remembering in the Digital World Through the Eye of the Media*, *in* THE ETHICS OF MEMORY IN A DIGITAL AGE: INTERROGATING THE RIGHT TO BE FORGOTTEN, *supra* note 5, at 9.

51. *Id.*

52. Edward L. Carter, *Argentina's Right To Be Forgotten*, 27 EMORY INT'L L. REV. 23, 36 (2013).

53. *Id.*

54. Lael J. Schooler & Ralph Hertwig, *How Forgetting Aids Heuristic Inference*, 112 PSYCHOL. REV. 610, 624 (2005); *see also* John T. Wixted, *The Psychology and Neuroscience of Forgetting*, 55 ANN. REV. PSYCHOL. 235, 264 (2004).

Individuals may desire the opportunity to redefine themselves, altering their "habits, political views, religion, make mistakes and have a fresh start."[55] Search engines often align results not according to their relevance in terms of timeliness. Each link appears to be equally valid. It is this concern that has grounded calls for an increased emphasis on forgetting being integrated to ICT systems. As Bannon outlines, the inaccessibility to be able to forget can disrupt everyday life.[56] Computing intelligence acts to recollect and archive behaviours and situations across the globe.[57] Bannon serves examples of e-mail being forwarded inappropriately to others and private messages being passed on without permission.[58] He notes that in counteracting the disadvantages that arise from a "surveillance society," designers should be concentrated with placing more control into users hands over their electronic space.[59] This could attempt to tackle a conflict between the human instinct to forget and a computing desire to comprehensively recall. With technological development, less emphasis is placed on user control of personal information.[60] Online memory exists to serve efficiency and its recollection function.[61] The right serves to not let the individuals present be unfairly contaminated by the past.[62] A final understanding is the importance of forgetting for society generally. In lessening surveillance woes, the right leads to greater personal freedom to live a fulfilling life.

D. Conclusion

The right is an umbrella term encompassing many possible policy aims and underlying privacy concepts. The concept of the individual having the right of oblivion with regard to negative elements in their past, a right of erasure, and objection regarding data controllers squared with Koops' three-prong analysis indicates a lack of consensus. A concern which runs right beside these concepts is the right of the public to have access to such information, freedom of expression, and public interest considerations.[63] Similar to the conceptualisation of privacy theory, there is a great deal of debate surrounding what the right actually is. Viewing

---

55. Carter, *supra* note 52.

56. Liam J. Bannon, *Forgetting as a Feature, Not a Bug: the Duality of Memory and Implications for Ubiquitous Computing*, 2 CODESIGN 3, 4 (2006).

57. *Id.* at 7.

58. *Id.* at 12.

59. *Id.*

60. *Id.* at 13.

61. *Id.*

62. *Id.*

63. *Id.*

the right to be forgotten as founded on personal autonomy and as a necessary behavioural response to modern privacy norms should guide future discourse. It is important to focus on what is at the core of the right.

From a viewpoint that values autonomy, there is merit in giving the individual control regarding information in the past that may negatively impact their future identity. The foundation of European data protection principles hands the individual more control over data processing.[64] The world as seen through the eyes of search engine results and social media is of a virtual construction that can sometimes have disproportionate consequences. A right to have information forgotten that is no longer relevant, incomplete, or leads to unreasonable harm is consistent with such foundations.

II. LEGAL FRAMEWORK UNDERLYING THE RIGHT TO BE FORGOTTEN

A. Data Protection and Privacy—Conflating Concepts

This Part seeks to analyse the current EU and ECHR (Convention) data protection framework and how the right will have positive implications for the future regime. The EU Charter of Fundamental Rights and Freedoms was given effect to by the Lisbon Treaty in 2009.[65] Article 7 of the Charter mirrors article 8, section 1, of the ECHR and provides respect for private and family life.[66] Article 8 on the other hand outlines protection of personal data.[67] The Court of Justice of the European Union (CJEU) cases illustrate a close relationship between personal data protection and privacy.[68] The Charter utilizes the ECHR as a floor, not a ceiling.[69] An emphasis on personal data protection within the Charter focuses on limiting improper usage of personal data by "increasing the right to transparency granted to each data subject."[70] The

---

64. Lindsay, *supra* note 23; *see* ELENI KOSTA, CONSENT IN EUROPEAN DATA PROTECTION LAW (2013).

65. Richard Clayton & Cian C. Murphy, *The Emergence of the EU Charter of Fundamental Rights in UK Law*, 5 EUR. HUM. RTS. L. REV. 439, 469-78 (2014).

66. *Id.* at 470.

67. *Id.*

68. GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 259 (2014).

69. Clayton & Murphy, *supra* note 65, at 469-78.

70. Yves Poullet & Serget Gutwirth, *The Contribution of the Article 29 Working Party to the Construction of a Harmonised Data Protection System: An Illustration of 'Reflexive Governance'?*, *in* HUMAN RIGHTS IN THE WEB OF GOVERNANCE: TOWARDS A LEARNING-BASED FUNDAMENTAL RIGHTS POLICY FOR THE EUROPEAN UNION 253 (Olivier de Schutter et al. eds., 2010).

ECHR does not have such equivalent protections.[71] The Charter's explicit reference to privacy and data protection give such independent constitutional status throughout all member states.[72] De Hert and Gutwirth suggest the Charter's right was introduced in order to bolster EU data protection legitimacy.[73] It does so in emphasizing the fundamental rights aspects of the Directive.

Post-Lisbon ratification, Advocate General Sharpston distinguished the right to privacy and data protection, stating, "Two separate rights are invoked: a classic right (the protection under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No. 108)."[74] The Court noted that the two rights were "closely connected" but treated them as "hybrid species" referring to "the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter."[75] Giving constitutional recognition to data protection as a separate right as opposed to being a subset of privacy is necessary. Data protection enshrines values not at the core of privacy such as "the requirement of fair processing, consent or legitimacy."[76] It also serves as a solution for democracies such as France and Germany who have no explicit privacy protection at a constitutional level.[77]

EU data protections are broader in scope than the ECHR equivalent.[78] The drafters of the EU framework left the provisions as broad as possible in an attempt to encompass all possible data that may concern individuals.[79] Lynskey argues that despite the ECHR adopting quite a broad interpretation as to the interpretation of privacy, it is not as expansive as the scope of the data protection principles.[80] One difference is that dissimilar to "privacy interference," the concept of "personal data"

---

71. *See id.*

72. *Id.*

73. Paul de Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, *in* REINVENTING DATA PROTECTION? 4-5 (Serget Gutwirth, Yves Poullet, Paul De Hert, Sjaak Nouwt & Cécile de Terwangne eds., 2009).

74. Orla Lynskey, *Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order*, 63 INT'L & COMP. L.Q. 569, 581 (2014).

75. Cases C-92109 and C-93/09, [Schecke v. Land Hessen], 2010 E.C.R. I-11063, at para. 71.

76. PRIVACY AND THE CRIMINAL LAW 81 (Erik Claes, Antony Duff & Serge Gutwirth eds., 2006).

77. *Id.* at 82.

78. *Id.* at 84.

79. Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Consteja Gonzalez" C-131/12, ART. 29 DATA PROTECTION WORKING PARTY (Nov. 26, 2014), http://www.pdpjournals.com/docs/88377 [hereinafter Implementation Guidelines].

80. *Id.*

is not context dependent.[81] Second, personal data encompasses data "to unidentified yet identifiable individuals."[82] Kuner has noted that the EU definition of data processing makes it difficult to comprehend "of any operation performed on personal data in electronic commerce which would not be covered by it."[83]

In a world of heightened surveillance, Lynskey concludes that a distinct right to data protection, as opposed to being a subset of privacy, is to be embraced.[84] Even though article 8 privacy is defined broadly enough to facilitate individual autonomy, rights such as self-determination and data portability are not yet established.[85] The asymmetric relationship between data controllers, processors and subjects underlines data protection mechanisms.[86] The disparity in balance between the power and control of the data subject compared to that of "industry and bureaucracy" means data protection has a broader remit than privacy.[87] Data protection hands the individual greater control in respecting individual self-determination, when compared to privacy under article 8. The conflation of data protection and privacy as it currently stands should be avoided. This lack of consensus undermines harmonization of the EU framework.[88] A distinct right of data protection focuses on the personality rights of the data subject and reduces power asymmetries.[89]

B. Towards a Data Protection Directive

In the 1970s, the Council of Europe believed article 8 contained a number of shortcomings with regard to technological developments.[90] An uncertainty surrounding what constituted "private life," combined with an emphasis on avoiding interference by public authorities resulted in a number of recommendations.[91] Directive 95/46/EC aimed to increase harmonization of national laws on data protection.[92] The

81. *Id.*
82. *Id.*
83. CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 74 (2007).
84. Lynskey, *supra* note 74, at 596-97.
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.*
90. Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, EUR. DATA PROTECTION SUPERVISOR (Sept. 15, 2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf.
91. *Id.*
92. *Id.*

Directive was hailed as creating a world leading privacy protection paradigm.[93]

Article 6.1 provides that once the purpose of collecting data has been fulfilled, such data is required to be deleted or be made anonymous.[94] The provision itself does not require the user to take any action and the data is presumed to be automatically removed.[95] This is a form of the right to be forgotten but in a more passive sense. In requiring the individual to take an active step, article 12 permits the user to obtain information from the controller confirming as to whether data related to them is being processed.[96] This requires the individual to request such data and subsequently evaluate its content.[97] Controllers are under an obligation to ensure that no more data is collected than is necessary for the required purpose.[98] Such data has to be accurate and kept up to date. Controllers have to take "reasonable steps" to ensure rectification or erasure where it is not accurate.[99] A right of erasure therefore arises where the controller fails in its obligations and disregards the individual's rights.

Article 14 creates a right to object to data storage.[100] Article 7 outlines a consent requirement, which has to be unambiguously given by the individual and explicitly so in the case of sensitive data.[101] The use of such mechanisms is lessened by what is referred to as the "household exemption."[102] In article 3.2 the provisions of the Directive are not applicable to "the processing of personal data . . . by a natural person in the course of a purely personal or household activity."[103] Ambrose and Ausloos have raised concerns with the Regulation, drawing attention to its limited scope.[104] It applies only "when the processing does not comply with the provisions of this Directive, in particular because of the

---

93. Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri, *Review of EU Data Protection Directive: Summary*, INFO. COMMISSIONER'S OFF. (May 2009), https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf.

94. *Id.*

95. *Id.*

96. SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 111 (Raf Casert trans., 2002).

97. Robinson, *supra* note 93.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. Noberto Nuno Gomes de Andrade & Shara Monteleone, *Digital Natives and the Metamorphosis of the European Information Society*, *in* EUROPEAN DATA PROTECTION: COMING OF AGE 134 (2013).

103. Directive 95/46/EC, *supra* note 35.

104. *Id.*

incomplete or inaccurate nature of the data."[105] The right to object is also of limited scope, only applying to matters relating to articles 7(e) and (f) and they have to be based upon "compelling and legitimate grounds."[106] *Google Spain SL* utilized article 12(b) concerning a right of rectification, erasure or blocking of data and article 14(b) a right to object, as the legal basis for the judgment.[107]

In January 2012 the Proposed Data Protection Directive explicitly refers to the right.[108] Two rights are explicitly referenced in the Draft Regulation, one of rectification within article 16, and a right to be forgotten within article 17.[109] The provision is stronger than the 1995 Directive in requiring the controller to carry out erasure without delay.[110] Controllers are required to do so unless the data is to be retained for freedom of expression purposes.[111] Implied consent can no longer be relied upon to process personal data.[112] Informed and explicit consent must be freely given.[113]

In cases where the controller has made the data public, they are under an obligation to inform third parties that such a right to be forgotten has been exercised, and will ask them to erase any links to or replications of such data.[114] This places quite an onus on third parties: cases may arise where such a third party has no knowledge of such existing copies or replications of the data.[115] The draft Regulation does not however give guidance as to how third parties are to comply with such a requirement and delete the content.[116] The provision however does not define what would constitute unauthorized publication.[117] Graux, Ausloos, and Valcke note that the provision only deals with publicized personal data, and does not accord for the unauthorized hidden processing of data, such as in cases of profiling and tracking.[118]

---

105. ELS J. KINDT, PRIVACY AND DATA PROTECTION ISSUES OF BIOMETRIC APPLICATIONS 729 (2013).

106. *Id.* at 667.

107. Case C-131/12, Google Spain SL v. Agencia Española de Datos, 2014 Q.B. 1022.

108. Directive 95/46/EC, *supra* note 35.

109. *Id.*

110. *Id.*

111. *Id.*

112. *See id.*

113. *Id.*

114. ELENI KOSTA, CONSENT IN EUROPEAN DATA PROTECTION LAW 253 (2013).

115. *Id.*

116. Directive 95/46/EC, *supra* note 35.

117. *Id.*

118. Hans Graux, Jef Ausloos & Peggy Valcke, *The Right To Be Forgotten in the Internet Era* 14 (Interdisc. Ctr. L. & ICT Research Paper No. 11, 2012), http://ssrn.com/abstract=2174896.

Providing a right to be forgotten in a situation where the information is shielded from public view is as important.

Stemming from a lack of conceptual consensus, there is a lack of clarity in the relationship between a right of erasure and to be forgotten. Recital 54 notes that to "strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties."[119] In this frame, the right to be forgotten is simply an extension of a right to erasure.[120] The provision does give further protection in the asymmetric relationship between the individual and the controller.[121] The data has to be deleted if it is no longer needed, second "if the data subject withdraws consent on which the processing is based." Third, if the individual objects to their information being used for marketing purposes it has to be removed.[122] Finally, if it is not processed in accordance with that data protection regulation, it is to be removed.[123]

C. ECHR Protections

Frantziou notes article 8 does not itself contain specific reference to protection of personal data.[124] article 8 has incrementally given regard to data protection.[125] Boehm opines that the European Court of Human Rights (ECtHR) regards the protection of personal data as a core part of an individual's right to respect for private and family life.[126] Until the 1990s, the ECtHR was reluctant to use data protection terms with reference to article 8.[127] Article 8 involves both a negative obligation in requiring the state to ensure the relevant rights are not interfered with,

---

119. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 11, COM (2012) 11 final (Jan. 25, 2012).

120. Gerrit Hornung, *A General Data Protection Regulation for Europe? Light and Shade In the Commission's Draft of 25 January 2012* 9 SCRIPTed 64, 74 (2012), http://script-ed.org/?p=406.

121. *See id.*

122. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, at COM (2012) 11 final (Jan. 25, 2012).

123. Hornung, *supra* note 120.

124. Eleni Frantziou, *Further Developments in the Right To Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, [*Google Spain, SL, Google Inc. v. Agencia Espanola de Proteccion de Datos*]*, 4 HUM. RTS. L. REV. 761, 761-77 (2014).

125. *Id.*

126. FRANZISKA BOEHM, INFORMATION SHARING AND DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY AND JUSTICE 25 (Serge Gutwirth et al. eds., 2012).

127. *Id.* at 28.

and a positive obligation involving designing measures to make sure the individual's rights are protected.[128]

Article 8 is open-textured, covering a wide breadth of issues that do not fall amongst other Convention provisions.[129] Strasbourg jurisprudence does not enshrine fundamental data protection principles.[130] Gutwirth cites cases such as *Klass, Leander, Amann, P.G. & J.H.* and *Perry* as illustrative of the Court going beyond the traditional conception of privacy involving intimate affairs.[131] Article 8 protects more than one would traditionally conceive as a general right to private life. The court interprets article 8 in an expansive manner, a "broad term not susceptible to exhaustive definition."[132] Personal autonomy is at the heart of article 8.[133]

The ECtHR has explored data protection through the scope of the right to respect for private life. Siemen concludes that the scope of data protection under the ECHR is the same as the right to respect for private life.[134] Convention No. 108 illustrates that in terms of subject matter, it must first concern information and second such information has to be personal.[135] Boehm summaries areas of data protection which fall under ECHR protection as telecommunications data,[136] personal information stored in public files,[137] DNA and fingerprint records,[138] personal information published on the Internet,[139] medical data,[140] and audio or video containing personal information.[141]

ECtHR data protection cases illustrate a gradual inclination towards separating data protection from private life.[142] In considering the

---

128. *Id.* at 26.

129. Karen Zarindast, *Google Glass—Augmenting Reality and Diminishing Human Rights?*, 26 ENT. L. REV. 6, 6-8 (2015).

130. De Hert & Gutwirth, *supra* note 73, at 14.

131. *Id.* at 59.

132. Peck v. United Kingdom, App. No. 44647/98, Eur. Ct. H.R. (2003).

133. Hilary Biehler, *The Right to Privacy and the Retention of DNA Profiles—Getting the Balance Right*, 5 EUR. HUM. RTS. L. REV. 439, 479-89 (2014).

134. BOEHM, *supra* note 126, at 28.

135. *Id.* at 30.

136. Liberty & Others v. United Kingdom, App. No. 58234/00, Eur. Ct. H.R. (2008).

137. Leander v. Sweden, App. No. 9248/81, Eur. Ct. H.R. (1987).

138. S & Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, Eur. Ct. H.R. (2008).

139. K.U. v. Finland, App. No. 2872/02, Eur. Ct. H.R. (2008).

140. Z v. Finland, App. No. 22009/83, Eur. Ct. H.R. (1997), M.S. v. Sweden, App. No. 10454/83, Eur. Ct. H.R. (1989).

141. Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (1978).

142. Copland v. United Kingdom, App. No. 62617/00, Eur. Ct. H.R. (2007); Liberty & Others v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (2008); K.U. v. Finland, App. No. 2872/02, Eur. Ct. H.R. (2008); Soderman v. Sweden, App. No. 5786/08, Eur. Ct. H.R. (2013).

relationship between the EctHR's balancing of Internet privacy and article 10, *Times Newspapers Ltd. (Nos. 1 and 2) v. The United Kingdom* outlined:

> The Court agrees at the outset with the applicant's submissions as to the substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free. The Court therefore considers that, while the primary function of the press in a democracy is to act as a "public watchdog," it has a valuable secondary role in maintaining and making available to the public archives containing news which has previously been reported.[143]

This grants substantive protection to third parties that can be considered "Internet archives" and make news and information available. *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* places a positive obligation on states to place an effective protection of freedom of expression for journalists on the Internet.[144] The case involved the publishing of a letter by a Ukrainian newspaper that accused senior local officials of criminal activity.[145] The newspaper noted that the letter may be false and its content was not verified. One of the officials concerned sought damages for defamation, leading to an award against the editorial board and editor in chief.[146] The Court noted that the risk of potential harm posed by the Internet with respect to human rights and freedoms is higher than the offline media.[147] The standards applicable therefore "have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned."[148] States must place an adequate framework to protect journalists' freedom of expression in the online world. On this basis, removing search results such as in *Google Spain SL* is a disproportionate step.

A line of recent cases illustrates the importance the Internet can act as a creative space for freedom of expression. In *Ahmet Yildirim v. Turkey*,[149] the applicant had been accused with insulting Ataturk's

---

143. Times Newspapers, Ltd. v. United Kingdom, App. Nos. 3002/03 and 23676/03, Eur. Ct. H.R. (2009).

144. Editorial Board of Pravoye Delo & Shtekel v. Ukraine, App. No. 33914/95, Eur. Ct. H.R. (2011).

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.*

149. Yildrim v. Turkey, App. No. 3111/10, Eur. Ct. H.R. (2012).

memory online. The Turkish Telecom Directorate subsequently applied for the extension that blocked access to Google Sites hosting the applicant's site. The applicant was unable to access his own site as a consequence.[150] The Court noted that blocking the avenue of accessing Google sites was "a restriction on Internet access which had the effect of also blocking the applicant's website."[151] The Court noted "since the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest."[152] The Turkish authorities had failed to meet the Conventions foreseeability requirement by failing to inform Google as to the site's removal.[153] It was an arbitrary measure violating article 10. Any unnecessary interference with freedom of expression on the Internet has to be subsequently supported by a strict legal framework. The Court discussed the right to Internet access as:

> Considered to be inherent in the right to access information and communications protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens. It can therefore be inferred from all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognized.[154]

An ECHR compliant right to be forgotten needs to be supported by a clear legal framework that correspondingly references competing considerations.

Frantziou terms *Wegrzynowski and Smolczewski v. Poland* the EctHR's "right to be forgotten ruling."[155] The case involved two journalists who wrote an article alleging that the applicants had acted in a corrupt manner in colluding with politicians.[156] The original Court ordered the journalists to make an apology and award compensation. The article subsequently appeared in the newspaper "*Rzeczpospolita*" and the applicants claimed continued publications violated their rights.[157] The Court subsequently ruled that the publication had relevant historical

150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. Frantziou, *supra* note 124, at 761-77.
156. Wegrzynowski v. Poland, App. No. 33846/07, Eur. Ct. H.R. (2013).
157. *Id.*

dimensions and compensation had previously been awarded. The ECtHR agreed, it confirmed that the Internet is a distinct method of communication and will "never be subject to the same regulations and control" as the printed media.[158] It subsequently poses potential harms to the exercise and enjoyment of privacy rights. Internet archives have an important function as a source of news and information.[159] Such archives are an important resource of historical reference. The principle that the press acts as a "public watchdog" was reiterated and that it has a valuable secondary role in "maintaining and making available to the public archives containing news which has previously been reported. . . . The maintenance of internet archives is a critical aspect of this role."[160] The Court referenced free speech considerations and the implications of removing links to Internet content:

> The Court accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputation.[161]

In *Delfi AS v. Estonia*[162] the Court mentioned that "the spread of the Internet and the possibility . . . that information once made public will remain public and circulate forever, calls for caution."[163] *Delfi* will be analysed and contrasted to *Google Spain infra* Part III.

D. CJEU's Foundation

Bodil Lindqvist[164] was a leading CJEU case surrounding data protection and what constitutes "personal or household activity."[165] The question the Court had to consider was whether publishing activities on a website were protected by the Data Protection Directive. The Directive does not apply to a natural person "in the course of a purely personal or household activity."[166] The Court felt however that this "must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the

158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*
162. Delfi AS v. Estonia, App. No. 64569/09, Eur. Ct. H.R. (2013).
163. *Id.*
164. Case C-101/10, Lindqvist v. Aklagarkammaren, 2003 E.C.R. I-12971.
165. Lee Andrew Bygrave, *Data Privacy Law and the Internet: Policy Changes*, *in* EMERGING CHALLENGES IN PRIVACY LAW: COMPARATIVE PERSPECTIVES 259, 267 (Normann Witzleb, David Linsay, Moira Patterson & Sharon Rodrick eds., 2014).
166. Directive 95/46/EC, *supra* note 35.

case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people."[167] The decision offers an expansive exploration of "processing." A simple act of placing information on a personal site comes under such "processing."[168] The broad decision sets the judicial texture for extending the data protection framework in *Google Spain SL*. The deferential direction of the decision is compared to *Van Hannover v. Germany (Princess of Monaco)* where a proportionality test was utilized ahead of the margin of appreciation.[169] The Court stated "the European constitutional order is still too thin to settle many of the heated conflicts among rights-holders that emerge routinely at national law."[170] In deferring to national law in matters concerning privacy and speech the Court "affirmed a European commitment to privacy and free expression and made a room for diverse moral orderings of public life at the national level."[171]

Second, *Varec* illustrates the CJEU interpreting privacy in a more expansive manner than the ECtHR.[172] The case involved a request by Varec to have details of a tender application, submitted by Diehl, in relation to a public tendering process.[173] The Court noted that disclosure of the documents would violate Diehl's rights under article 8.[174] The Court drew upon jurisprudence such as *Colas Est* and *Peck* in coming to this conclusion.[175] In an expansive notion of private life the court held that "it follows from the case law [of the ECtHR that] the notion of "private life" cannot be taken to mean that the . . . commercial activities . . . of legal persons are excluded."[176] Groussot and Gill-Pedro outline how *Colas Est* was not concerned with private life, but with respect for domicile and home of a corporation.[177] The EctHR's conception as to the protection of private life and the home are quite

---

167. *Id.* at 47.

168. ANDREW MURRAY, INFORMATION TECHNOLOGY LAW: THE LAW AND SOCIETY 499 (2013).

169. Van Hannover v. Germany, App. No. 40660/08 and 60641/08, Eur. Ct. H.R. (2012).

170. Francesca Bignami, *Constitutional Patriotism and the Right to Privacy: A Comparison of the European Court of Justice and the European Court of Human Rights*, *in* NEW TECHNOLOGIES AND HUMAN RIGHTS 128, 241 (Therese Murphy ed., 2009).

171. *Id.* at 244.

172. Case C-450/06, Varec SA v. Belgian State, 2008 E.C.R. I-00581.

173. Xavier Groussot & Eduardo Gill-Pedro, *Old and New Human Rights in Europe*, *in* SHAPING RIGHTS IN THE ECHR 256 (Eva Brems & Janneke Gerards eds., 2013).

174. *Varec SA*, 2008 E.C.R. para. 48.

175. Peck v. United Kingdom, App. No. 44647/98, Eur. Ct. H.R. (2003); Société Colas Est v. France, App. No. 37971/97, Eur. Ct. H.R. (2002).

176. SHAPING RIGHTS IN THE ECHR, *supra* note 173, at 256.

177. *Id.*

different. The facts of *Peck* which involved an individual who was experiencing mental health difficulties being filmed carrying a knife in a public place, are different to the tendering process in *Varec*.[178] The CJEU takes an expansive approach in utilizing ECtHR jurisprudence to interpret rights and freedoms. Utilizing article 8 jurisprudence in the CJEU's adjudication of privacy issues is to be welcomed.

Third, with the accession to the Charter in 2009, the Court has begun to take an increasingly emboldened stance.[179] In *Digital Rights Ireland*[180] contrary to the Advocate General's Opinion, the Court found that the Data Retention Regulation 2009 was unlawful. In *Opinion 2/13* Advocate General Kokott recommended that the draft agreement on accession to the ECHR should be found lawful if certain amendments were undertaken.[181] The Court decided that accession was incompatible with EU law. The decision was met with substantial criticism.[182] Following this, *Google Spain SL* in 2014 was a further example of the Court's bold approach. *Schrems*[183] is the Court's most recent highly publicized privacy and data protection case. With this increased regard for privacy rights, it decided, in the wake of Snowden revelations, that the EU-U.S. safe-harbour program was inadequate.[184]

A distinct right to data protection incorporates elements that help realize the right to be forgotten. Such ingredients include; a right to withdraw previously given consent to process data; the right to object to data processing; the duty to delete or anonymise data once the purpose has been achieved and the right to erase data where its processing is noncompliant with protection requirements.[185] The right to be forgotten involves broader informational autonomy elements such as; the right to change one's mind regarding data previously disclosed or which consent has been given; the right to not be permanently reminded of one's past; to not have the past disproportionately harm the future; the right to have

---

178. *Id.*

179. Orla Lynskey, Conference Presentation at the University of Cambridge: EU Internet Regulation After *Google Spain* (Mar. 27, 2015).

180. Cases C-293/12 and C-594/12, Digital Rights Ireland v. Minister for Commc'ns, 2014 E.C.R. I-593.

181. *Id.*

182. *Id.*

183. Case C-362/14, Schrems v. Data Protection Comm'r, 2005 E.C.L.I. 627.

184. Schrems is the most recent illustration of this emboldened approach. Having regard to European data protection and the effects on individual rights when data is transferred to third countries where protections are inadequate, the EU/U.S. safe harbor agreement was deemed invalid.

185. *See* Cecile de Terwangne, *The Right To Be Forgotten and Informational Autonomy in the Digital Environment*, *in* THE ETHICS OF MEMORY IN A DIGITAL AGE: INTERROGATING THE RIGHT TO BE FORGOTTEN, *supra* note 5.

data deleted as it is no longer legitimate to be kept; and a right to refuse de-contextualisation of data by tackling the power of Internet search engines, whilst accepting that the data will remain in its initial context.[186]

E. Conclusion

This section has sought to analyse the EU and ECHR framework that underlines the right to be forgotten. The Convention itself does not currently contain sufficient protection. Issues have been worked through in a piecemeal fashion. Such inadequacies can partly be resolved by giving clear regard to data protection within the Convention. Along with such reform, it is believed the Court should embrace the right to be forgotten. Inadequacies in the current legal framework illustrate a need for creative solutions. The right has positive implications in mapping modern ECHR privacy norms. The EU framework gives constitutional recognition across all member states to the importance of data protection principles. Both the EU and ECHR regimes can learn a great deal from existing positives and negatives to carve effective privacy protection in the future.

III. IMPLICATIONS OF THE RIGHT TO BE FORGOTTEN

A. Google Spain SL

Google Spain SL has provoked more academic commentary than any other case in data protection in the last sixteen years.[187] Consteja González had two articles published about him in Spanish newspapers.[188] These related to real estate auction proceedings that were initiated by social security debts.[189] In 1998, the newspaper as required by Spanish law published the article, but the information subsequently resurfaced in 2009.[190] Because the information became more accessible through Google's search engine, the applicant submitted that it was no longer relevant.

Roughton notes there were three key questions to be considered: (1) to what scope could national courts make an order which would affect

---

186. *See id.*

187. Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, *in* DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? 213, 213-24 (Hielke Hijmans & Herke Kranenborg eds., 2014).

188. *Id.*

189. *Google Spain SL*, at para. 14; TAKIS TRIDIMAS, THE GENERAL PRINCIPLES OF EU LAW 374 (Albertina Albors-Llorens, Kenneth Armstrong & Marxus W. Gehring eds., 2013).

190. CONSTANCE E. BAGLEY, MANAGERS AND THE LEGAL ENVIRONMENT: STRATEGIES FOR THE 21ST CENTURY 816 (2016).

activities of corporations whose operations and seat were not in the EU, (2) what encompasses "data processing" in the case and how does one identify a data "controller," and (3) how much can the data subject object to the data controller's behaviour.[191] Advocate General Jääskinen's opinion dealt with such.[192] First, regarding article 4(1)(a) of the EU Data Protection Directive 95/47/EC, a "controllers" processing of personal data is carried out in the context of the activities of its "establishment," "when the undertaking providing the internet search engine sets up in a Member State, for the purposes of promoting and selling advertising space on the search engine, an office or subsidiary which orientates its activity towards the inhabitants of that State."[193] Second, an Internet search engine provider that contains information by third party web sites, "processes" data with regard to article 2(b) of Directive 95/46 where it is of a personal nature.[194] Third, the provisions of the Directive, involving a right of erasure, right to object within article 14(a) and blocking through article 12(b), do not give the individual a right to prevent the search engine from indexing content which is legally published on a third parties" site.[195] Jääskinen did not view Google as processing the data in question and not a "controller." The complaint concerned previously published content that was no basis for an action against Google. Jääskinen outlined that the right to object to search engines results is inconsistent since it only indexed materials that were already on the Internet.[196] Because the material is already available on the Internet itself, a right to be forgotten could be said to be of limited use.

If the CJEU had opted to follow the Advocate-General, the case would have generated limited attention.[197] The CJEU discussed two form of indexing. First, indexing was less objectionable if it concerned "secerned items of data."[198] The Court secondly considered aggregation—where multiple instances of information regarding the same matter carries increased weight in comparison to a single item.[199] The search

191. Ashley Roughton, *Google and the "Right To Be Forgotten"—Setting the Record Straight*, 14 PRIVACY & DATA PROTECTION 6, 6-7 (2014) (subscription required).

192. Case C-131/12, Google Spain SL v. Agencia Espanola de Protección de Datos, 2014 Q.B. 1022.

193. *Id.*

194. Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines* 214 (LSE Legal Studies Working Paper No. 3, 2014), http://ssrn.com/abstract=2496060.

195. *Google Spain SL*, 2014 Q.B. 1022.

196. Roughton, *supra* note 191, at 6-7.

197. *Id.*

198. *Id.*

199. *Id.*

information returned is of a structured nature that affects the subject's privacy rights. In the absence of such a search engine, finding personal information would be a more difficult task. The decision places Google under no obligation to erase an unstructured single return.[200] However, a single unstructured result could still raise privacy concerns and require takedown.

A second issue is to the scope of the right to erasure and that of the right to be forgotten. Articles 12(b) and 14(a) of the Data Protection Directive provide data subjects with a right of erasure, blocking, and rectification or to object.[201] The right is of a subjective nature.[202] It concerns the data subjects desire to have the information bypassed if they consider it to be prejudicial. The links which the search engine provides are also "previously and lawfully" published by third parties. If publishers do not want the materials to be included in the indexing of results, they can remove them. Jääskinen did not believe that articles 12(b) and 14(1) created a right to be forgotten, "[T]he Directive does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests."[203] It was believed that creating such a right with regard to the functioning of search engines would have a distorting effect.[204]

> [It] would need to put itself in the position of the publisher of the source web page and verify whether dissemination of the personal data on the page can at present be considered as legal and legitimate for the purposes of the Directive. In other words, the service provider would need to abandon its intermediary function.[205]

The Advocate General opinion placed freedom of expression ahead of privacy considerations. Jääskinen warned against inferring such a right from the current EU privacy framework, creating such a right could encroach upon freedom of information.[206] The Advocate General's opinion was pragmatically reasoned, yet failed to consider the broader privacy implications in how Google acts as an information monopolist.

---

200. *Id.*

201. Directive 95/46/EC, *supra* note 35.

202. Paula Herrero Prieto, *Search Engines: Interplay of Fundamental Rights and Principle of Proportionality*, 20 COMPUTER & TELECOMM. L. REV. 213, 213-21 (2014).

203. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 Q.B. 1022.

204. Prieto, *supra* note 202.

205. *Google Spain SL*, 2014 Q.B. 1022.

206. *Id.*, at paras. 126-133.

Contrary to expectation, the CJEU embraced the right, albeit in a dysfunctional manner. It began by considering whether a search engine could constitute a "controller" and if it involved the "processing of personal data." The Court relied on *Bodil Lindqvist* in finding that the "loading of personal data on an internet page must constitute 'processing.'"[207] A search engine locates information published by third parties, indexes it on an automatic basis, stores it temporarily and distributes to its users.[208] It is when the search engine "stores," "organises," "discloses," or "makes available" personal data that it falls under the ambit of article 2(b).[209] The Court was not persuaded by Google's submission that it did not distinguish between personal and other data.[210] It also rejected the argument that knowledge of the data was required.[211] The Court found that since it determines the purpose as well as means of the processing it conducts, it was a "controller."[212] A broad interpretation of "controller" was adopted. A distinction was given between the original publication of content and the search engines processing it.[213] Google's overall control of the search process meant it determined access to the original publication and it was not an intermediary. The Court distinguished between a website and a search engine, Google's interests were solely economic and consequently could not rely upon the article 9 journalistic exception.[214]

Google submitted that the processing in this case was not carried out in the activities of Google Spain Inc.[215] The CJEU found that the activities of the search engine operator and those of the "establishment" were "inextricably linked."[216] The Court believed that the search engine service was related to the selling of advertising space.[217] The advertising

---

207. Elizabeth Kelsey, Google Spain SL and Google Inc. v. AEPD and Mario Costeja Gonzales*: Protection of Personal Data, Freedom of Information and the "Right To Be Forgotten*,*"* 4 EUR. HUM. RTS. L. REV. 319, 395-400 (2014).

208. *Id.*

209. *Id.*

210. *Id.*

211. *Id.*

212. *Id.*

213. Steven James, *The Right to Privacy Catches Up with Search Engines: The Unforgettable Decision in* Google Spain v. AEPD, 20 COMPUTER & TELECOMM. L. REV. 130, 130-33 (2014).

214. Herke Kranenborg, *Google and the Right To Be Forgotten*, 1 EUR. DATA PROT. L. REV. 1 (2015).

215. Brendan van Alsenoy & Marieke Koekkoek, *The Extra-Territorial Reach of the EU's "Right To Be Forgotten,"* (Interdisc. Ctr. L. & ICT, Working Paper No. 20/2015, 2015).

216. *Id.*

217. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.M.L.R. 27 para. 56.

function "constitute[s] the means of rendering the search engine . . . economically profitable."[218] The Court also paid attention to the fact that the EU framework sought to prevent individuals from circumventing protection in applying a broad territorial scope.[219] The CJEU suggests the effects principle (usually thought of in the competition law context) provided justification for exercising jurisdiction. Alsenoy and Koekkoek note how the Court repeatedly referred to the "effective and complete" protection of individuals.[220] The opinion is influenced by the "substantial effect" Google's search engine activities have on data subjects.

The third and fourth questions considered by the CJEU dealt with the right.[221] The provisions of the Directive, combined with articles 7 and 8 of the Charter of Fundamental Rights guarantee the protection of personal data and the right to private life.[222] The CJEU noted that article 12 of the Directive enables the individual to obtain rectification, blocking and erasure of data that is not compliant.[223] Article 6 was referenced as requiring personal data to be processed in a fair and lawful manner.[224] Article 7(f) considers the elements that make data processing legitimate.[225] The Court noted that this "necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from articles 7 and 8 of the Charter."[226] Notably absent from the inquiry is article 11 of the Charter and article 10 of the ECHR.

Information that is initially posted may over the course of time become incompatible with the Directive. This is because the data is no longer necessary with regard to the purpose for which it was initially collected. The Court gave strong recognition to articles 7 and 8 of the Charter, which have primacy over the economic interests of the search engine and the general public interest.[227] The processing of data related to the individuals name through a search engine can put such rights at risk:

> It enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the Internet—information which potentially concerns a vast number of

218. *Id.*
219. *Id.* para. 54.
220. Van Alsenoy & Koekkoik, *supra* note 215, at 9.
221. *Google Spain SL*, 2014 E.M.L.R. 27.
222. Robinson, *supra* note 93; *see* Directive 95/46/EC, *supra* note 35.
223. *Google Spain SL*, 2014 E.M.L.R. 27 para. 20.
224. *Id.* para. 7.
225. *Id.* para. 8.
226. *Id.* para. 74.
227. *Id.* para. 97.

> aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty—and thereby to establish a more or less detailed profile of him.[228]

Where the public interest no longer requires the information, the subject should have the opportunity to have the link suppressed. It was specifically mentioned that the availability of the right would depend on the individual's role in "public life."[229] The Court failed in expanding when this "preponderant interest" would require access to the information. The Court ultimately concluded that the display of the applicants name leading to links to archives of newspapers detailing his social security debts from sixteen years ago, were no longer relevant.[230] The applicant had a right to not have such information linked to him by means of search engine results.[231]

The judgment allows the individual to have links containing their name removed where "having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine."[232] The Court does not refer to the term "right to be forgotten" in its ruling, but it mentions it in its judgment.[233] The decision allows the user to request de-indexed or to not be included in search results. It does not wipe the information from the virtual slate. In making personal information more difficult to access, it acts as a limited tool. The Court did reference that the removal of links would affect the legitimate interests of Internet users.[234] The data subject's rights trump the Internet users" desire to access content. The right is not absolute and a balancing of the competing rights has to be undertaken.[235] It is only in the situation where the individual is a "public figure" that the interest will overcome, but this was not satisfactorily expanded upon.

1. Analysis

The decision is insular in focus.[236] The Courts judgment style has been described as "overly abstract, vague and elliptical" and "cryptic

228. *Id.* para. 80.
229. *Id.* para. 81.
230. *See id.*
231. *See id.*
232. *Id.* para. 94.
233. Kuner, *supra* note 187.
234. Prieto, *supra* note 202.
235. *Google Spain SL*, 2014 E.M.L.R. 27.
236. Kuner, *supra* note 187, at 15.

[and] Cartesian."[237] In discussing data protection there is no reference to international human rights instruments such as the ECHR. Given the global nature of the Internet, it is unfortunate the Court did not give regard to international documents or institutions.[238]

Frantziou points out two fundamental errors in the judgment.[239] First, the Court failed to engage with the content of the right to privacy: second the Court failed to engage with the ECHR.[240] On the first point, the Court did not actually complete any detailed assessment of the right to privacy. The Court did pay reference to the impact that search engines like Google could have on the Individual's private life.[241] The Court failed to determine in what circumstances interference would violate articles 7 and 8 of the Charter.[242] Unanswered questions remain relating to the application of the Charter to private actors. It is true that if the Court utilizes articles 7 and 8 to engage a right to be forgotten for the data subject, it has to firstly explore the content of such rights.[243] The mere identification of rights, rather than interpreting their content, contrasts to article 8 ECHR cases.

There was also a failure to conduct a proportionality inquiry. The applicants desire to have the information removed has to be squared with a number of elements. There is no distinction between the various fundamental rights and freedoms within the Charter itself.[244] Article 8 of the Charter concerning the protection of personal data is the central right concerned, however a number of others are also relevant. Article 8 is not "an absolute right, but must be considered in relation to its function in society."[245] Such a right does not automatically trump other competing rights or freedoms. Article 11 of the Charter recognizes freedom of expression, corresponding to article 10 of the ECHR. Article 11(1) also protects the right to receive ideas and information.[246] Article 16 of the Charter protects the freedom to conduct business.[247] Allowing the data subjects right to have the information removed, because it is no longer relevant, without consideration as to these competing interests is best avoided.

---

237. *Id.*
238. *Id.*
239. Frantziou, *supra* note 124, at 761.
240. *Id.*
241. *Google Spain SL*, 2014 E.M.L.R. 27., para. 80.
242. Frantziou, *supra* note 124, at 767.
243. *Id.*
244. Prieto, *supra* note 202, at 21-32.
245. *Id.*; Case C-92/09, Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, para. 48.
246. Prieto, *supra* note 202, at 213-21.
247. *Id.* at 219.

The ECHR permits freedom of expression exceptions, but such "must be narrowly interpreted and the necessity for any restrictions must be convincingly established."[248] Third-party publishers upload content with the knowledge that search engines like Google will actively index. Access to the content can be increased through search engine functionality. The third party has an option to opt out of the indexing process. Publisher's freedom of expression in displaying the content within the search results is at issue. Further, article 11(1) involves the individual's right to receive ideas and content. By providing increased access to the flow of information search engines engage in article 10 protected freedom of expression. The ECtHR has noted that "particularly strong reasons must be provided for any measure limiting access to information which the public has the right to receive."[249] Search engines have an important role in the dissemination of content. Transparency of information is important in an open democracy. Deletion of links impacts on freedom to access content. Constraints on information access need to be carefully examined in light of the public interest.

Article 16 also needs to be considered *Belgische Vereniging van Auteurs, Componistan en Uitgevers CVBA v. Netlog NV* is a case on point.[250] The case concerned the freedom to conduct business of hosting service providers and the intellectual property rights by copyright holders.[251] The Court held that an injunction would lead to an infringement of the host service in conducting its enterprise.[252] The Court noted that the procedure involved would (1) mandate the provider to put in place a costly, complicated and permanent computer system at its own cost; (2) not comply with the fair balance requirement; (3) the granting of the injunction would infringe the fundamental rights of the servers users, including the freedom to "receive or impart information."[253] Google's business model was secondary to privacy rights.

In assessing whether the measure is proportionate, EU courts consider whether it is necessary and appropriate in achieving the objective, where other measures are available the least onerous one is

---

248. Gaweda v. Poland, App. No. 26229/95, Eur. Ct. H.R. (2002), para. 32 (citation omitted).

249. Wegrzynowki v. Poland, App. No. 33846/07, Eur. Ct. H.R. (2013), para. 57 (citation omitted).

250. Case C-360/10, Société Belge des Auteurs, Compositeurs et Editeurs v. Netlog, Celex No. 610CJ0360 (2012).

251. *Id.*

252. *Id.* para. 51.

253. *Id.* paras. 46-48.

used.[254] If the first requirement is not satisfied, the page of origin containing the information will still publicly exist.[255] Deleting the original web content would achieve the aim. There are less onerous means of achieving the desired result. The publisher engaging in an "opt-out mechanism" from indexing would prevent the material being accessed on any search engine. It would also lead to a more non-discriminatory decision with respect to Google. The search engine bears an impossible burden. Google is arguably taking the role of publisher in assessing whether the information is legitimate. The Advocate General believed that given the complex nature of the matter and the rights concerned, the right should not be exercised. This imposes a disproportionate burden on the search engine, which could lead to the possibility of censorship by a private party.

Frantziou refers to the ECHR within the case as the "dog that did not bark."[256] Reference to how the ECtHR has dealt with "internet archives" in cases such as *Times Newspapers* and *Wegrzynowski and Smolczewski* would have been welcomed. Advocate General Jääskinen stated:

> [A]rticle 8 thereof also covers issues relating to protection of personal data. For this reason, and in conformity with article 52(3) of the Charter, the case law of the Court of Human Rights on article 8 . . . is relevant both to the interpretation of article 7 of the Charter and to the application of the Directive in conformity with article 8 of the Charter.[257]

A lack of reference creates a presumption that the right requires a higher threshold for the human rights protection, compared to the ECHR minimal standards.[258] A failure in working out the relationship between articles 7 and 8 of the Charter with article 11 relating to freedom of expression substantiates such concerns. Such questions raise concern as to the institutional competence of the CJEU in interpreting fundamental rights provisions. In avoiding broader considerations, the Court should avoid "withdrawing into one's own constitutional cocoon, isolating the international context and deciding the case exclusively by reference to international context and deciding the case exclusively by reference to internal constitutional precepts."[259]

---

254. Prieto, *supra* note 202, at 217-20.

255. *Id.*

256. Frantziou, *supra* note 124, at 882.

257. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.M.L.R. 27, para. 115.

258. Frantziou, *supra* note 124.

259. Kuner, *supra* note 187, at 17.

The decision concerns large-scale Internet search engines. It defined a search engine as "a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference."[260] This definition encompasses the main search engine operators such as Bing and Yahoo, but Kuner questions whether the definition can extend to providers who undertake search services.[261] He believes that a broad conception is necessary to include a multiplicity of online services that have search functions.[262] Social networks and commercial databases have search engine functionality. The Court did refer to the objective of the Data Protection Directive as "ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data."[263] In interpreting this broadly, Kuner believes that the judgment can be extended from Internet search engines to a variety of online services that have search functionality.[264] Extension of the right beyond delisting to commercial and governmental databases would be effective in ensuring access to the right. In principle it sets in place a regime to be enforced against bloggers, ratings websites, news archives, and social networking.[265]

In holding a private corporation with such dominance as Google subject to fundamental rights provisions, it presents the way forward in holding private actors to account for violating privacy norms. The Court properly takes into account the power Google holds as the "master switch" in the online world. In recognizing this role and the impact it can have on the individual, it gives greater protection for potential privacy breaches. In identifying the "public interest" exception, the Court correctly identifies potential problems of de-indexing. Items that remain within the public interest will remain in the search results. The judgment recognizes Google does not merely act as in "intermediary" regarding content, but impacts on privacy. Google is also not required to carry out active monitoring of indexing of whether content is incompatible with data protection mechanisms. Google is only required to take action with

260. *Google Spain SL*, 2014 E.M.L.R. 27, para. 21.
261. Kuner, *supra* note 187, at 8.
262. *Id.*
263. *Google Spain SL*, 2014 E.M.L.R. 27.
264. Kuner, *supra* note 187, at 8.
265. David Erdos, *The General Shape of EU Internet Regulation after Google Spain: David Erdos*, YOUTUBE (Apr. 17, 2015), https://www.youtube.com/watch?v=6v_UFY65aEK.

respect to notices it receives concerning particular content, similar to a notice and take down system.

2. Google's Compliance

There are concerns regarding Google's competence to implement the decision. In November 2014, the article 29 Data Protection Working Group released an opinion on the right's implementation.[266] It clarifies that the ruling firstly only applies to search engine operators who act as data controllers. It does not apply to the original website where information relating to the individual is published.[267] The search engines economic interests will not serve as justification to interfere with the individual's rights.[268] It is important to create a balance between the two. The data subject should give sufficient information when making the request. This includes an explanation of the reasons why removal is requested, identification of the specific URLs and whether they fulfil a role in "public life."[269] The European Commission believes that in search engines assessing requests on a case-by-case basis, "this assessment must balance the interest of the person making the request and the public interest to have access to the data by retaining it in the list of results."[270] But no discussion illuminates what factors private companies should take into account in determining whether the link should be deleted.

Data protection authorities will focus on instances where there is a link between the individual and the EU legal regime. Limiting access to the right to operators who have a EU domain is illogical. It is possible to circumvent de-indexing by using google.com, rendering implementation ineffective.[271] Where the content, subject, or audience is of European focus, where it is viewed should determine applicability of the decision, rather than the domain extension. This undermines giving individual's further control. Using the facts of *Google Spain SL* as an example it is clear to see why implementation should be worldwide. The announcement was published by a Spanish newspaper, the website was

266. Implementation Guidelines, *supra* note 79.

267. *Id.* at 2.

268. *Id.*

269. *Id.* at 7.

270. *Myth-Busting, the Court of Justice of the EU and the "Right To Be Forgotten*," EUROPEAN COMM., http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet-rtbf_mythbusting_en.pdf (last visited Oct. 11, 2015).

271. Julia Powles, *Results May Vary*, SLATE (Feb. 25, 2015, 10:38 AM), http://www.slate.com/articles/technology/future_tense/2015/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html.

hosted by a server in Spain, it concerned a Spanish citizen.[272] In such a case it would be permissible for the Spanish authorities to grant a global order.

It is noted that the individual may use the template form given by the search operator, but if the individual chooses not to use such mechanisms, the search engine should not refuse the relevant request. The Working Group Guidelines do not reference article 12 or article 14 upon which *Google Spain SL* founded the right.[273] The Guidelines recognize that the criteria are a "flexible working tool" that will be applied on the foundation of national legislation.[274] The individual should have access to the right through any adequate means. Sufficient information and explanations have to be provided by the individual applicant and the search engine. Transparency in how Google is currently dealing with requests is problematic. The mechanism through which takedown is achieved needs to be illustrated. At the moment, the process operates on an arbitrary basis. The search operator should also not disclose to users that information has been removed relating to an individual's name. Google currently indicates that search results may have been removed due to data protection requests. Commentary on the future of guidance procedures finds that overall regime looks towards increasing the rights of individuals.[275] The right to be forgotten is not an automatic one, discussions surrounding the draft Regulation illustrate that its legitimacy is far from settled.[276] Corporations who fall under the decision and subject to requests should put in place transparent mechanisms and guidelines. Such procedures would comply with existing data protection law but also that of the article 29 Working Group guidelines.

Making private entities "judge, jury and executioner" of the right creates clear problems. The decision places a significant onus on such operators to transparently implement the ruling. Given the difficulties courts face in trying to balance the various competing interests, giving private corporates, such as Google, discretion to make these decisions is unprincipled. Affording Google a power to decide whether to remove

---

272. Brendan Van Alsenoy & Marieke Koekkoek, *The Territorial Reach of the EU's "Right To Be Forgotten": Think Locally, but Act Globally*, EJIL: TALK! (Aug. 14 2014), http://www.ejitalk.org/the-territorial-reach0of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/.

273. *See* Implementation Guidelines, *supra* note 79.

274. *Id.* at 5.

275. Nuria Pastor, *Deconstructing W29 RTBF Guide and a Look to the Future*, FIELDFISHER (Feb. 2, 2015), http://www.fieldfisher.com/publications/2015/02/deconstructing-wp29-rtbf-guide-and-a-look-to-the-future.

276. *Id.*

content awards unwavering discretion. At time of writing, Google has evaluated more than 1.15 million URLs for removal, with more than 325,000 requests received.[277]

3. Impacts

The creation of new rights is a complex and often controversial process. The right to be forgotten already has its foundations in European data protection legislation and ECHR jurisprudence. Given the competing considerations required in order for the right to be exercised, there are numerous situations in which exercising such a right could be potentially "inappropriate and in some cases even absurd" due to public interest and freedom of expression considerations.[278] The right should be exercised on an *ultima ratio* basis, a measure of final resort where other legal tools provide inadequate.[279] This is a sensible framework as the right can be most effectively accessed where other legal tools are exhausted.

A "cascade of decaying information" involves a series of legal tools providing a proportionate remedy balanced with the relevant competing interests.[280] Where one of the existing legal remedies does not provide sufficient protection, one moves to the next measure. The right to be forgotten is the final gear in the chain. This helps to alleviate some of the criticisms that the right is obscure and has censorship potential. The privacy landscape is shifting rapidly. The right helps in alleviating some of the privacy concerns emerging with technological innovation. Both private and public actors are gaining increased access to capture information. Formulating sufficient privacy safeguards requires creativity. Carolan has noted, "The scale of technological change in recent years has created substantial disparities in the way in which different groups engage in different technologies."[281] With technological developments, individuals have decreased control over information concerning them. The manner in which data is recorded and gathered is

277. *European Privacy Requests for Search Removals*, GOOGLE, http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en (last updated Oct. 30, 2015).

278. Oskar Josef Gstrein, *The Cascade of Decaying Information: Putting the "Right To Be Forgotten" in Perspective*, 21 COMPUTER & TELECOMM. L. REV. 40, 40-48 (2015).

279. *Id.*

280. *Id.*

281. Eoin Carolan, *Surveillance and the Individual's Expectation of Privacy Under the Fourth Amendment*, 71 CAMBRIDGE L.J. 250, 253 (2012).

not as restricted as it was before, governments and commercial entities retain data continuously.[282]

Even though the right emerges at a haphazard level within *Google Spain SL*, its theoretical foundations deal with fundamental concerns involving consumer's privacy in the future legal regime. When one considers how the 1995 Directive could never have anticipated innovations such as Google, a broad based right with an anchor in autonomy has long-term advantage. Where there may be a gap between the existing legal framework and the vindication of privacy rights, the right is of use. Rosen has critiqued that "Europeans have a long tradition of declaring abstract privacy rights in theory that they fail to enforce in practice."[283] With unforeseeable future privacy concerns, the right is an important tool. Where the individual wishes to have information forgotten, the first potential stage in the "cascade of decaying information" is rectification. Rectification involves correcting data inaccuracies. Where factual inaccuracies are present, rectifying inaccuracies will suffice. If rectification of the information does not provide a sufficient remedy, one moves to a right to deletion or erasure. Rectification may not be appropriate since the individual may object to disclosure of the information itself.

Erasure places a responsibility on the controller to erase information from its interface. These two methods involve managing information, whereas "delisting" or "de-indexing" involves limiting accessibility to such content. Search engines operate as the online "master-switch" directing the user to content. Google has a dominant position in the search engine industry and is currently subject to a European Commission investigation for alleged anticompetitive conduct.[284] Where results relating to the individual create disproportionate harm to the relative public interest, a right of "delisting" is appropriate. This is not a right to be forgotten, but does assist in limiting accessibility. Exercising a right of erasure could also help in ensuring access to the final step, the right to be forgotten. The right to be forgotten itself requires comprehensive deletion of information compared to de-indexing.

---

282. Stephen Mason, *The Internet and Privacy: Some Considerations*, 21 COMPUTER & TELECOMM. L. REV. 68, 68-84 (2015).

283. Rosen, *supra* note 16.

284. Julia Powles, *Europe Is Targeting Google Under Antitrust Laws but Missing the Bigger Picture*, GUARDIAN (Apr. 15, 2015, 11:47 AM), http://www.theguardian.com/technology/2015/apr/15/europes-targeting-google-under-antitrust-laws-missing-bigger-picture.

Where such steps do not provide an appropriate remedy, the right should be available. All of the stages are however forms of the right to be forgotten. The final stage involves comprehensive takedown of content and this restricts dissemination. Gstrein's assertion that one cannot expect the information to be completely wiped away from a wide variety of information systems has merit.[285] This echoes the feeling of the House of Lords EU Home Affairs, Health and Education Sub-Committee report, Baroness Prashar commented:

> The expression, "right to be forgotten" is misleading. Information can be made more difficult to access, but it does not just disappear. Anyone anywhere in the world now has information at the touch of a button, and that includes detailed personal information about people in all countries of the globe. Neither the 1995 Directive, nor the CJEU's interpretation of it, reflects the incredible advance in technology that we see today. We believe that the judgment of the Court is unworkable.[286]

It is challenging to comprehensively erase all references to particular content online. However, strident attempts can still be made to lessen access to harmful content. In terms of a broader "right to be forgotten," the fact that it will be impossible to have all content suppressed does not make it completely "unworkable." The CJEU's conception of the right is problematic. The onus that it places on search operators is overly expansive, rendering implementation impossible. In the absence of independent oversight and clear guidelines as to implementation, the current right is defective. If the right to be forgotten is to be implemented by search engines its full underlying capabilities, values and supporting normative arguments will not be effectively achieved. It is believed that extensions are necessary in the ambit of the rights reach, beyond de-indexing in *Google Spain SL*. Problems of implementation do not mean "de-indexing" should be disregarded. In order for the individual to have effective recourse, limiting access and availability to the content assists in achieving the rights ambitions.

At this final stage, where all previous remedies provide are ineffective, the original third-party content may need to be erased. *Google Spain SL* in some situations provides a "band aid" solution. Because the search result is removed only on the European domain site, content will still be easily accessed through the .com domain.[287]

---

285. Gstrein, *supra* note 278.

286. *EU Data Protection Law: A 'Right To Be Forgotten'?*, U.K. HOUSE OF LORDS REPORT (July 30, 2014), http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf.

287. *Id.*

Additionally, the content remains on the original page.[288] The permanency of online content combined with the speed at which it can spread, means that removing the search results does not always protect the interests underpinning the right. Information will only be taken down where it mentions the individual's name.[289] This can be easily bypassed by searching using other relevant names or the surrounding circumstances. Confining its application to the individual's name is not effective. A more holistic approach considering how the content relates to the individual's welfare would be beneficial. In order to effectively suppress the content itself, requiring the original source page to remove the content would be the most effective method. This shifts the onus away from search engines on to the original content holders. It also has to be considered that the individual can use such global search engines to find information regarding them online that is illegal or irrelevant. Search engines give the individual the mechanism to run checks on their online profile. Search engines can have enormous impact on individual image. A right of de-listing decreases accessibility and assists in achieving the right's ambitions.

A closed model network is one where "every set of data can be labelled and indexed and is therefore removable in its entirety."[290] A shift of focus in situations concerning personal information to be contained within closed networks would help in having it properly categorized and removed completely. This is consistent with Koops' "deletion in due time" element.[291] A move towards a closed model landscape could impact the creativity of the Internet and freedom of expression for both the user and content holders. This would create challenges to ECHR compliance. Such closed model networks would be particularly helpful in online banking, health care systems or online governmental services involving citizens' data.[292] Perhaps complete erasure can only be achieved in such closed model situations. The challenges facing comprehensive erasure do not trump the rights potential benefits.

In concentrating on awarding greater control to the individual, requiring third parties to remove content where the harm is disproportionate to the relative public interest would be welcomed. Control primarily vests in the hands of third parties currently, the right attempts to balance this asymmetric relationship. Enforcement would

288. *Id.*
289. *Id.*
290. Gstrein, *supra* note 278, at 46.
291. *See* Koops, *supra* note 9, at 245.
292. Gstrein, *supra* note 278, at 47.

occur through national Data protection authorities, with courts offering an appeal mechanism. The future implementation of the right is not completely "unworkable," but difficult.

I now turn to analysing the rights impacts for (1) the individual, (2) institutions, (3) corporations, and (4) states.

B. Individuals

A behavioural understanding of the right indicates how is a necessary response to privacy concerns.[293] Developments in online advertising, cloud computing and the globalization of data have led individual's desire greater control over their online presence. Modern technologies are persistent with searchability and sharing features often interwoven, little emphasis is placed on individual control. Advances provide new avenues through which oppressive governments and employers can gather and store information about individuals.[294] Mitrou comments on how Internet archives through cached copies and search engine abstracts can provide a distorted representation of the individual: "The default of forgetting has changed into a default of remembering."[295] Personal data is now a valuable currency being used to fund free services like social networks, news sites and search engines.[296] A damaged or mischaracterized virtual identity can have long-lasting consequences for social status and future employment. With individual actions facing being shared with an unlimited global audience, the individual may alter their participation in social and public life.[297] An effective illustration of this is the emergence of "revenge porn," for example, where a disgruntled ex-partner gathers intimate photos or videos and publicly uploads the content to the Internet. Giving victims such a right awards an effective remedy as opposed to solely prosecutions.[298] The

---

293. Kirsty Hughes, *A Behavioural Understanding of Privacy and Its Implications for Privacy Law*, 75 MOD. L. REV. 697 (2012).

294. LEE BURGUNDER, LEGAL ASPECTS OF MANAGING TECHNOLOGY 452 (2011).

295. Lilian Mitrou, *EU's Data Protection Reform and the Right To Be Forgotten—A Legal Response to a Technological Challenge?*, 5TH INT'L CONF. OF INFO. L. & ETHICS (Feb. 5, 2012), http://ssrn.com/abstract=2165245.

296. Maria Giannakaki, *The "Right To Be Forgotten" in the Era of Social Media and Cloud Computing*, *in* HUMAN RIGHTS AND RISKS IN THE DIGITAL ERA: GLOBALIZATION AND THE EFFECTS OF INFORMATION TECHNOLOGY 10 (Christina M. Akrivopoulou & Nicholas Garipidis eds., 2012).

297. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

298. Lilian Edwards, *Revenge Porn: Why the Right To Be Forgotten Is the Right Remedy*, GUARDIAN (July 29, 2014, 12:07 PM), http://www.theguardian.com/technology/2014/jul/29/revenge-porn-right-to-be-forgotten-house-of-lords.

suppressing of links to such content would give the individual another legal remedy to combat harmful content.

Popular discourse has concentrated on the right as having the effect of rewriting historical archives, silencing unfavourable criticism or reputation grooming. The right is centrally concerned with placing a veil of obscurity on information as it becomes inadequate or irrelevant to the public interest. The right puts brakes on the uncontrolled collection of personal information.

A society concentrated with sharing online, diminishes individual capacity for intimacy. Altman and Taylor's social penetration theory is particularly interesting in this context, the unforgiving and persistent nature of online communication limits individual control on the flow of information.[299] There is limited gradual development of individual personality within the online sphere. Due to social media sites, an individual can learn a substantial amount about a person before meeting them. A relevant example here is smartphone applications and personal data. Individuals regard their phone as private and will be reluctant to share its use with others.[300] Users "feel violated" when it is revealed that applications are accessing data without active knowledge.[301] Repeated interference with privacy creates negative psychological consequences and difficulty in regaining control in information management.[302] Solove draws a distinction between risk management and access control.[303] Consumers desire control over personal information and a commitment from commercial operators that they will limit privacy risks once data is no longer within their direct control.[304] Risk management for the individual becomes increasingly difficult the longer that data is stored.

Given this asymmetric relationship combined with decreased control of personal information, the right has legitimacy. Before modern technology, information could simply fade into the archives allowing individuals to prevent past mistakes defining future existence. Where the mistake or sin was so great, the individual could simply move elsewhere and escape. The online world however is an unforgiving place. Giving

---

299. IRWIN ALTMAN & DALMAS TAYLOR, SOCIAL PENETRATION: THE DEVELOPMENT OF INTERPERSONAL RELATIONSHIPS (Holt, Rinehart & Winston, Inc., eds., 1973).

300. Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skuladottir & Hoskuldur Borgthorsson, *Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use*, ACM CHI CONFERENCE HUMAN FACTORS COMPUTING SYS. 2347 (2014), http://www.scott.mainzone.com/pubs/14-leakiness-creepiness.pdf.

301. *Id.* at 1248.

302. *Id.*

303. Daniel Solove, *A Taxonomy of Privacy*, 154 UNIV. PENN. L. REV. 477 (2006).

304. *Id.*

individuals a second chance is an important value. Nowadays, such mistakes are easily found through search engine results, the individual should have access to having inaccurate or irrelevant content erased.[305] There are positive implications for the individual in providing additional protection and recourse, especially in situations where personal information is unlawfully used. The right allows the individual to manage and construct their online identity. Human behaviour has changed profoundly with technological advancement, privacy concerns have increased and this requires renewed legal tools. What would have been considered traditionally private events can now be easily found within the public domain. Those who do not know the surrounding context can easily judge the individual.[306] Recognizing the importance of forgiveness in the digital age is necessary and the right achieves this need. In recognizing commercial operators decreased regard for informational self-determination, the right forms the basis of a renewed legal regime concentrated on greater control.

C. Institutions

Section two focused on working through the EU and ECHR legal backdrop to the right. The case illustrates the CJEU's inadequacy in adjudicating fundamental privacy and freedom of expression provisions. *Google Spain SL* is part of the EU's broader regulatory data protection reform. It may have been more effective for the EU regime to outline the scope and basis of the right, rather than the CJEU attempting to create a right to "delisting" or a broader right to be forgotten with limited foundations. The decision could be viewed as an example of judicial creativity. In a twenty-page judgment, it created an ambitious and necessary extension of European data protection law. It sets the scene for a Court not afraid to strengthen privacy protections, notwithstanding political critique. *Google Spain SL* arose during negotiations over new legislation in the form of the draft General Data Protection Regulation.[307] It helps in focusing discussion on balancing the privacy rights of the individual with the "preponderant public interest." It is hoped the case draws attention to the rights of the data subject within finalized discussions.

---

305. Matt Bishop, Emily Rine Butler, Kevin Butler, Carrie Gates & Steven Greenspan, *Forgive and Forget: Return to Obscurity*, *in* PROCEEDINGS OF THE 2013 WORKSHOP ON NEW SECURITY PARADIGMS WORKSHOP 1, 7 (2013).

306. *Id.*

307. Joseph Jones, *Control-Alter-Delete: The "Right To Be Forgotten,"* 36 EUR. INTEL. PROP. REV. 547, 595-601 (2014).

Sartor provides a useful examination as to the Draft Regulation's contents.[308] He concludes that the Regulation only introduces incremental alterations, rather than effectively introducing the right.[309] It provides a process for termination of data processing where retention becomes unlawful. Article 17 requires "controllers who made personal data public" to make contact with third parties who process the data, this is unclear. Placing obligations on controllers to engage third parties to erase data is indeterminate. Similar issues arise as to Google's implementation of de-indexing requests, how can third parties enforce the right in an objective and independent manner. A provider is immune from liability if "it does not have actual knowledge of illegal activity or information and, as regards claim for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent."[310] Sartor believes the exceptions to the right are "redundant" as lawful processing is excluded.[311] The Regulation does not clarify the circumstances in which providers of content in the online world will be subject to the right. The Regulation does not provide certainty as to whether failing to remove a request would oblige the provider to compensate the data subject.[312] The assessment of balancing freedom of expression parameters with the data subject's privacy is a complex process. The uncertainty within the Regulation will only fuel tensions surrounding the right's controversy. With proposed fines of up to 1% of global annual turnover, it places enforcement of the right to be forgotten on par with competition law.

Second, I wish to examine how the introduction of a right to be forgotten could impact on the judicial interpretation of privacy rights. The protection of journalistic freedom and the Internet archives in cases such as *Times Newspapers* and *Editorial Board of Pravoye Delo and Shtekel* place freedom of expression over privacy. Removing search results interferes with categorizing and archiving online content. It would be beneficial for court's to embrace the concept in judicial thinking. Given the open-textured nature of article 8, the concept would fit into the EctHR's constituent rights landscape.

In *Weller* the Queen's Bench Division found that the photographing of Paul Weller's children on a family day out breached article 8.[313] The

---

308. Giovanni Sartor, *The Right To Be Forgotten in the Draft Data Protection Regulation*, 5 DATA PRIVACY L. 64, 64-72 (2015).

309. *Id.* at 72.

310. *Id.*

311. *Id.* at 67.

312. *Id.* at 69.

313. Weller & Ors v. Associated Newspapers, Ltd., 2014 E.W.H.C. 1163.

Court awarded £5,000 to the older child and £2,500 to each of the twins.[314] The Court did not grant an injunction since it was accepted that the defendants would not publish the photographs again, however a subsequent judge did grant an injunction, as there was evidence the unlawful publication would be repeated.[315] In time to come, if the images of the children were to resurface, the right to be forgotten would provide a suitable legal tool. Given the open nature of the Internet, the right is a more vigorous tool in preventing dissemination. In *Mosley v. News Group Newspapers Ltd.*, the Court found a breach of the applicant's rights to confidentiality and privacy.[316] Given how fast images spread in the online sphere, the right would be appropriate where the relative privacy harm outweighs legitimate public interest. Justice Eady refused the applicants request for an interim injunction preventing further publication of the story, "the material was so widely accessible that an [injunctive] order . . . would have made very little practical difference" and "the dam has effectively burst."[317] Similarly, in the *Spycatcher* litigation, since the content was already in the public domain, an injunction would have been of limited value.[318] Where information is already in the public domain, it is worth remembering the comments in *Aleksey Ovchinnikov*:

> [I]n certain circumstances a restriction on reproducing information that has already entered the public domain may be justified, for example to prevent further airing of the details of an individual's private life which do not come within the scope of any political or public debate on a matter of general importance.[319]

The Paris Tribunal de Grande Instance held in 2013 that Google had to automatically filter a number of images relating to Mosley from its operation.[320] If the pictures are illegal and a breach of privacy norms, steps should be taken to limit availability. Freedoms of expression considerations are sometimes trumped by privacy rules. Damages are not completely effective in cases of online harm, the individual desires

---

314. Stephen Foster, *Press Photographs: Protecting the Privacy of Celebrities and Their Children*, 19 COM. L. 73, 86-92 (2014).

315. *Id.*

316. Mosley v. News Grp. Newspapers Ltd., 2008 E.M.L.R. 20 (U.K.).

317. *Id.* para. 36.

318. URSULA SMARTT, MEDIA & ENTERTAINMENT LAW 63 (2014).

319. Ovschinnikov v. Russia, App. No. 24061/04, Eur. Ct. H.R. (2010).

320. *Max Mosley Sex Pictures Should Be Blocked by Google French Judge Order*, HUFFINGTON POST, http://www.huffingtonpost.co.uk/2013/11/06/max-mosley-google_n_4226785.html (last updated June 11, 2013).

reducing accessibility to the content itself. Giving the individual a clean slate enables them to move forward in life.

Mr. Mosley had further success in the District Court of Hamburg where the Court noted "the images violate the specially protected privacy of the plaintiff . . . to a very considerable extent, as they provide information about sexual acts.[321] In that regard, they are likely to lead to the stigmatization of the plaintiff, and "[i]t should be noted that a particularly high degree of intervention regularly emanates from the pictorial representation of the sexual behaviour of a person, since the viewer actually has the scene 'before his eyes.'"[322] The High Court has recently allowed a similar claim to proceed.[323] In rebutting counsel for Google's contention that the claim was unsubstantiated, Justice Mitting found the claimant had a viable case.[324] The Court cited *Google Spain SL* in holding Google as a "controller."[325] This would have provided a useful opportunity for the High Court to provide further examination of the right. The case may have resulted in an article 267 TFEU reference, through with the CJEU would have clarified areas that *Google Spain SL* left opaque. Mosley would likely have been considered a public figure and the "preponderant interest" outlined in *Google Spain SL* would require retention of the search results. The parties subsequently settled, and the discussion as to the "public interest" exception did not arise.

On the existing jurisprudence of the ECtHR, it is important to note some further implications. The Court places primacy on the importance of preserving the Internet archives. It is believed that an ECHR challenge to *Google Spain* is theoretically possible. On the basis of *Times Newspapers* and *Wegrzynoswki* the Court would regard protecting unhindered access to Internet content and the Internet archives as fundamental. *Von Hannover (No. 2)* illustrates a number of criteria to be considered when balancing freedom of expression and privacy.[326] Both article 8 and 10 are of equal value and a margin of appreciation is afforded to national courts in balancing the competing interests.[327] There

---

321. Dominic Crossley, *Case Law, Hamburg District Court:* Max Mosley v. Google Inc., INFORRM INT'L F. RESPONSIBLE MEDIA BLOG (Feb. 5, 2014), https://inforrm.wordpress.com/2014/02/05/case-law-hamburg-district-court-max-mosley-v-google-inc-google-go-down-again-this-time-in-hamburg-dominic-crossley/.

322. *Id.*

323. Mosley v. Google Inc. & Google UK Ltd., 2015 E.W.H.C. 59 (U.K.).

324. *Id.* para. 54.

325. *Id.* para. 19.

326. *Id.* paras. 11, 104.

327. Van Hannover v. Germany, App. Nos. 40660/08 and 60641/08, Eur. Ct. H.R. (2012).

was initially no reasonable public interest in Mr. Gonzalez's life.[328] However, given the global media coverage surrounding his particular case, he will remain in the collective memory. His case is permanently linked to a legal landmark that will be impossible to have erased. The search results providing information to users are an integral part in categorizing information within the Internet archives. It is believed the Court would find removal of such links to be disproportionate given freedom of expression considerations.[329] The case and his particular circumstances have generated considerable public interest. Search engines contribute to the media acting as a "public watchdog." A balancing exercise between the applicants article 8 privacy rights and the rights of other to receive the information, will in many cases revoke de-indexing. The Court may award a wide margin of appreciation to states when balancing privacy and freedom of expression. However, *Google Spain SL*'s de-indexing with respect to Mr. Gonzalez would appear to contravene ECHR jurisprudence. If an applicant like Mr. González makes an anonymous application under article 35 § 2(a) of the admissibility criteria, this would assist limiting public interest in his particular circumstances and lessening a need for de-indexing.[330]

A recent Dutch ruling said *Google Spain SL* "is not meant to remove articles which may be unpleasant, but not unlawful, from the eyes of the public via the detour of a request for removal to the operator of a search machine."[331] An effective balancing exercise will assist in determining whether the removal is disproportionate, content which is not unlawful may need to be removed where privacy harms trump the public interest. The ordinary citizen should have access to the right. Lee notes "an unpopular politician, a poorly reviewed physician, and a paedophile were among the first to have issued Google removal requests."[332] In such cases the public interest will clearly require retention. If discussion surrounding the right concentrated on how the right affords

---

328. Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.M.L.R. 27 para. 98. Accordingly, because in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of article 12(b) and subparagraph (a) of the first paragraph of article 14 of Directive 95/46, require those links to be removed from the list of results).

329. *Id.*

330. *Id.*

331. Robin Hopkins, *Google Spain, Freedom of Expression and Security: The Dutch Fight Back*, PANOPTICON (Mar. 13, 2015), http://www.panopticonblog.com/2015/03/13/google-spain-freedom-of-expression-and-security-the-dutch-fight-back/.

332. NEWTON LEE, FACEBOOK NATION: TOTAL INFORMATION AWARENESS 145 (2014).

increased autonomy to the innocent citizen, overall benefits in its introduction will be increasingly realised.

Wegrzynoswki was coined the EctHR's "right to be forgotten" case; however, in drawing parallels to *Google Spain SL*, *Delfi* requires note.[333] Notwithstanding the fact that the site had taken down the comments upon notification, the Court found that it should have prevented unlawful comments from being posted. The ruling places an impossible burden on websites with interactive comment sections. The Court did not accept Delfi's abuse report button or automatic word-based filter were sufficient to circumvent publication of defamatory content.[334] The website had substantial control over the comments published and was not merely a "passive service provider."[335] Similarities can be observed between this and how the CJEU found that Google is not merely an intermediary, but a "controller" of content. This is correct as Google controls a vast amount of information. The processing of data which search engines undertake is additional and different to that of publishers.[336] Weinert advises that website owners who have such comment sections should put in place a system where the user can actively retain control and delete content after submission.[337]

Guillemin notes how *Delfi* fundamentally failed to properly deal with intermediary liability.[338] The Court failed to apply the E-Commerce Directives hosting liability provisions which gives incentives to online platforms like Delfi to remove content when notified of illegality, in such cases immunity arises.[339] Delfi removed the content on the same day of notification. The decision places an undue burden on sites with comment areas. It may lead to pre-emptively closing such sections and limiting users access to information. The Court was overtly concerned with protecting individual rights against Internet companies, but failed to realise how this would impact users freedom of expression. In a recent Northern Irish decision *J19 and J20 v. Facebook Ireland*, Judge Gillen asked counsel to consider *Delfi*'s applicability.[340] It was believed the case

---

333. Delfi As v. Estonia, App. No. 64569/09 Eur. Ct. H.R. (2013).

334. Eileen Weinert, *Oracle at "Delfi"—European Court of Human Rights Holds Website Liable for Angry Reader Comments*, 25 ENT. L. REV. 28, 28-31 (2014).

335. *Id.* at 30.

336. Prieto, *supra* note 202, at 213-21.

337. Weinert, *supra* note 334, at 30.

338. Gabrielle Guillemin, *Case Law, Strasbourg:* Delfi AS v. Estonia*: Court Strikes Serious Blow To Free Speech Online*, INFORRM INT'L F. RESPONSIBLE MEDIA BLOG (Oct. 15, 2013), https://inforrm.wordpress.com/2013/10/15/case-law-strasbourg-delfi-as-v-estonia-court-strikes-serious-blow-to-free-speech-online-gabrielle-guillemin/.

339. *Id.*

340. Eileen Weinert, J19 and J20 v. Facebook Ireland, 25 ENT. L. REV. 110, 110-12 (2014).

had a "shrinking sense of relevance" to the relevant matter, however it "may well be fact sensitive and indeed subject to an appeal to the Grand Chamber."[341] Given its inadequacies, it is welcomed that the trial judge dismissed the relevance of *Delfi*. Clear difference is observed in the type of information removed in *Delfi* and *Google Spain SL*. *Google Spain SL* does not require the information to be abusive or defamatory.[342] If the content is simply irrelevant a takedown request can be made. *Delfi* is moreover concerned with potentially abusive content, however the relevant comments would not have been considered defamatory under U.K. law. Unfortunately, the Grand Chamber mostly followed the Court's reasoning. The judgment fundamentally failed to answer whether *Delfi* was an ISP or a media publisher. Weinert ultimately concludes that "this is a decision which can only be explained by a reluctance of the ECtHR to interfere with Estonia's margin of the appreciation, when it really ought to have. Small comfort that the courts of England and Wales would not have and have not ruled on this issue in the same way.[343]

Under *Delfi*, if *Google Spain SL* were to come before the ECtHR, a shift appears from a concentration on preserving the Internet archives and freedom of expression, to recognizing Google as not merely a "passive provider." The CJEU was correct in finding that Google is not a "neutral intermediary." It has an obligation to de-index unlawful or irrelevant content when it is brought to attention.[344] It should be noted that search engines have automatic algorithms, this makes it difficult to determine which content is to be included. Given this automated process, Advocate General Jääskinen believed Google could not ensure all information complies with articles 6, 7 and 8 of the Directive. The Court held that search results involve "a structured overview of the information . . . that can be found on the Internet . . . and which, without the search engine, could not have been interconnected or could have been only with great difficulty—and thereby to establish a more or less detailed profile."[345] Search engines help to ensure the free flow of information. They are not a hosting service, caching or mere-conduit

---

341. *Id.*

342. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.M.L.R. 27, para. 115.

343. Eileen Weinert, Delfi As v. Estonia*: Grand Chamber of the Court of Human Rights Hands Down its Judgment: Website Liable for User-Generated Comments*, ENT. L. REV. 246, 246-250 (July 2015); Delfi As v. Estonia (64560109) (2014) 58 E.H.R.R. 29 (ECHR).

344. Nico Zingales, *Virtues and Perils of Anonymity: Should Intermediaries Bear the Burden?*, 5 J. INTELL. PROP. INFO. TECH. & E-COMM. 1, 26 (2014).

345. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.M.L.R. 27, para. 80.

service, and do not fall within the intermediary liability regime of articles 12-15 of the E-Commerce Directive.[346] Whether search engines fall within the intermediary exemptions of the E-Commerce Directive has not been dealt with, leading to confusion. *Google Spain SL* failed to discuss intermediary liability. It did note however that Google was of a different nature to website platforms.[347] Given the differences in intermediary liability between a search engine like Google and an online platform like Delfi, the decisions overall impact is limited.

Similarities exist in the indeterminacy *Delfi* creates and how Google is to correctly put in place a mechanism to objectively "de-index" links. Its overall value is limited in assessing how the right to be forgotten would be treated before the ECtHR. Kuczerawy concludes that the existing EU framework on notice and taken down "incentivises over-compliance and interference with fundamental human rights."[348] *Delfi* negates transparency and proportionality, intermediaries are unable to determine which notices they should accept or disregard. This enables arbitrary or overcautious procedures.

Conclusions in the EU regulatory reform process should provide insight as to the extent the right will be broadened and enforced beyond "de-indexing." Second, the right is to be welcomed as a further judicial tool in protecting privacy rights within the ECHR. Time will tell in what circumstances individual privacy will trump public interest and freedom of expression parameters.

C. Corporations

Businesses that are engaged in the processing of data online, could be considered a "controller" and subject to the ruling. Corporations that have large databases or search functionality built into their interfaces should review policies in light of developments. An entity could simply use a .com domain and avoid impact. The ruling can be easily circumnavigated by pointing the domain name away from the EU. Information or content that is placed on sites from third parties also needs to be reviewed as to its compliance with data protection rules. If a business considers itself to be a "controller" it should take steps to ensure

---

346. Aleksandra Kuczerawy & Jeff Ausloos, *NOC Online Intermediaries Case Studies Series: European Union and Google Spain*, INTERDISCIPLINARY CTR. L. & ICT (ICRI), KU LEUVEN (Feb. 18, 2015).

347. *Google Spain SL*, 2014 E.M.L.R. 27.

348. Aleksandra Kuczerawy, *Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative*, 1 COMP. L. & SECURITY REV. 31, 46-56 (2015).

compliance. Google was found to be a controller even though it argued it only organized data. This means businesses that do not change personal data, but exercise some amount of control over it, could be classified as a controller.

A core problem with the decision is its failure to anticipate what constitutes effective compliance. The decision stated "the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified."[349] It is unclear what exactly satisfies this. Google set up a form for individual's to submit a de-listing request, similar to a notice and takedown procedure. Bing and Yahoo have followed Google's example.[350] *Delfi* would place an increased obligation on sites to actively take down conduct that appears to be abusive. If information becomes irrelevant, entities will be required to put in place procedures that deal with content where it becomes incompatible with time. It is believed a notice and takedown approach is favoured rather than independent deletion. Another ambiguity concerns what will be considered valid competing interests for businesses when engaged in a balancing exercise. A failure to work through these considerations could lead businesses to rethink undertaking trade in the EU. With such uncertainties comes increased risk of litigation. Businesses will have to train individuals to be able to meet requests in a transparent and cost-efficient manner. A broader additional implication is that businesses using Google as their online search engine may decrease. As de-listing requests increase businesses will have reduced access to fuller results. The ruling has the potential to overall increase costs requiring efficient systems be put in place to ensure compliance.

From the individual data subjects perspective, the introduction of the right greatly benefits subjecting corporations who process and control personal information to greater scrutiny. The decision makes corporations tread with increased care when interfering with privacy rights. In taking a broader interpretation of search functionality, social media sites such as Facebook and Twitter that have internal search mechanisms could be subject to the ruling. As Smith comments "Human

---

349. *Google Spain SL*, 2014 E.M.L.R. 27, para. 72.

350. Andrew Griffin, *Microsoft and Yahoo Join Google in Deleting Search Results Under Right To Be Forgotten Ruling*, INDEPENDENT (Dec. 1, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-and-yahoo-join-google-in-deleting-search-results-under-right-to-be-forgotten-ruling-9896100.html (last visited Sept. 15, 2015).

memory fades, but without a right of erasure, social networks will never forget."[351]

D. States

The Investigatory Powers Tribunal recently found that British intelligence services unlawfully accessed millions of individual personal communications collected by the National Security Agency (NSA).[352] In *Klass* it was noted that "[d]emocratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction."[353] The judiciary does play a key role in holding the state to account for privacy violations. The existence of legislation that permits secret monitoring interferes with article 8. Unlawful means of surveillance include wiretapping an individual's dwelling and interception of electronic communications.[354] Putting in place sufficient legal structures to combat infringements increases public confidence and serves as deterrence. Any legislation permitting surveillance has to be clear enough to enable the citizen to determine the circumstances in which the state will engage in secret collection of data. Reidenberg has commented the collection of data and government purchase of data threatens democracy in creating a "transparent citizen, but a non-transparent government."[355] The debate over the right illuminates such issues and further empowers data subjects in seeking to delete information the state holds which is irrelevant or illegal. Where legitimate and proportionate public interest or security requires retention, the request can be refused. Introduction of the right will have clear impact on large databases controlled by government bodies. Existing data protection and freedom of information remedies will usually provide sufficient redress. However, where such tools do not achieve the desired

---

351. Kathryn Smith, *The Right To Be Forgotten: Legislating for Individuals To Regain Control of Their Personal Information on Social Networks*, REINVENTION: INT'L J. UNDERGRADUATE RES. (2014), http://www.2.warwick.ac.uk/fac/cross_fac/reinvention/issues/volume7issue1/smith/.

352. Owen Bowcott, *UK-US Surveillance Regime Was Unlawful for Seven Years*, GUARDIAN (Feb. 6, 2015, 5:10 PM), http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa.

353. Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (1978), at 18.

354. BOEHM, *supra* note 126, at 36.

355. Joel Reidenberg, Conference Presentation, Privacy Rights and Wrongs: Balancing Moral Priorities for the 21st Century (Apr. 21, 2009).

result or in the future become redundant, the right to be forgotten may be appropriate.

A central criticism of the right has been allegations that states will use it as a vehicle of censorship. Effective implementation of the right will mean that it will not be an instrument of censorship. The Commission notes "the right to be forgotten does not allow governments to decide what can and cannot be online or what should or should not be read."[356] The right may enable citizens to attempt to remove unfavourable traces of their past, however it does not facilitate government censorship. Increasing transparency in the manner at which search engines undertake the takedown process, will assist in confronting censorship quarrels. Additionally, the Commission states that data protection authorities will provide oversight, providing an appeal mechanism.[357] The problems in how search engines are to effectively implement the right have to be firstly addressed.

IV. CONCLUSION

This piece has sought to frame the right to be forgotten as a necessary legal mechanism. It promotes positive implications for individual autonomy and self-determination. *Google Spain SL* can be admired for the Court's judicial activism. It is "an imperfect decision in an imperfect world."[358] Clear criticisms are to be observed in its application. It does lay the foundation for a right of considerable importance for the consumer in the future. Dave Eggers book "The Circle" captures a world in which keeping information to oneself is a selfish act. In such a society deletion is illegal, "Secrets are lies. Sharing is Caring. Privacy is theft."[359] It may take significant time before the right becomes effectively operational and is largely dependent on conclusions in the EU reform process.

The first Part of this work observed there is a current lack of consensus in terminology surrounding the right, phrases like erasure,

---

356. Lorna Woods, Delfi v. Estonia*: Curtailing Online Freedom of Expression?*, BLOGPOST EU L. ANALYSIS, http://eulawanalysis.blogspot.ie/2015/06/delfi-v-estonia-curtailing-online.html (last visited Nov. 5, 2015) (reasoning that the *Strasbourg* court put Delfi in a position of effectively having to monitor user content).

357. *Mythbuster: The Court of Justice of the EU and "the Right To Be Forgotten,"* EUROPEAN COMM'N (Sept. 18, 2014), http://ec.europa.eu/justice/newsroom/data-protection/news/140918_en.htm.

358. *Conference Report: Google's Pain, an Imperfect Decision in an Imperfect World*, BINDMAN'S (Apr. 2015), http://www.bindmans.com/news-and-events/publications-and-update/conference-report-googles-pain-an-imperfect-decision-in-an-imperfect-world.

359. Betsy Morals, *Sharing Is Caring Is Sharing*, NEW YORKER (Oct. 30, 2013), http://www.newyorker.com/tech/elements/sharing-is-caring-is-sharing.

oblivion, deletion, rectification and delisting repeatedly surface. Any framework of such a right of oblivion, erasure or forgetting has to include an inquiry as to the competing freedom of expression and public interest considerations, relative to the potential privacy harms. Viewing the right as grounded on personal autonomy and as a necessary behavioural response to modern privacy norms should guide future discourse. The second Part illustrated shortcomings in both the EU and ECHR frameworks underlining the right. The ECtHR comprehensively engages in balancing the competing rights provisions compared to the CJEU. However, the lack of a distinct right to data protection undermines individual protection. The third Part illustrated failures in *Google Spain SL* to properly engage with the right to privacy, an effective proportionality inquiry and the absence of a strict legal framework underlining the right. The final Part outlined the benefits of introducing the right primarily for the individual and how it impacts judicial institutions, states, and corporations.