

2017

Sir, the Radar Sir, It Appears to Be . . . Jammed: The Future of “The Right to Be Forgotten” in a Post-Brexit United Kingdom

Cory DiBene

Follow this and additional works at: <http://digital.sandiego.edu/ilj>

 Part of the [International Law Commons](#)

Recommended Citation

Cory DiBene, *Sir, the Radar Sir, It Appears to Be . . . Jammed: The Future of “The Right to Be Forgotten” in a Post-Brexit United Kingdom*, 19 *San Diego Int'l L.J.* 161 (2017)

Available at: <http://digital.sandiego.edu/ilj/vol19/iss1/7>

This Comment is brought to you for free and open access by the Law School Journals at Digital USD. It has been accepted for inclusion in *San Diego International Law Journal* by an authorized editor of Digital USD. For more information, please contact digital@sandiego.edu.

Sir, the Radar Sir, It Appears to Be . . . Jammed: The Future of “The Right to Be Forgotten” in a Post-Brexit United Kingdom

CORY DIBENE*

“To improve is to change; to be perfect is to change often.” –

Winston Churchill

TABLE OF CONTENTS

I.	INTRODUCTION	162
II.	THE ORIGIN OF THE “RIGHT TO BE FORGOTTEN” IN THE EU.....	164
III.	IMPLEMENTATION OF THE “RIGHT TO BE FORGOTTEN” AND THE UK’S RESPONSE	174
IV.	BREXIT ANALYSIS AND THE FUTURE IMPACT ON “THE RIGHT TO BE FORGOTTEN” IN THE UNITED KINGDOM.....	179
V.	WHY THE UNITED KINGDOM WILL CONTINUE TO FOLLOW THE “RIGHT TO BE FORGOTTEN” POST-BREXIT	191

* © 2017 Cory DiBene. J.D. 2018 Candidate, University of San Diego School of Law. I would like to thank everyone involved at the University of San Diego School of Law for the incredible support throughout the publication process. This Article was selected in mid-2017 for publication, and there have undoubtedly been many uncontrollable legislative developments in this rapidly changing area of law by the time of actual publication in 2018. I hope this Article demonstrates the complex underpinnings formulating the interplay of Brexit, the law, and technology.

I. INTRODUCTION

Virtually all information nowadays lives online and potentially for an eternity. Global societies are catching up to the reality that everything said or done has the potential to be recorded and accessed online on mega-servers. Thus, the value of protecting data has created a modern Gold Rush amongst data miners, each of whom vie to be the first and best to fortify online informational systems.

Imagine present-day online informational systems as a vehicle: in the driver seat of this vehicle is capitalism, putting a virtual pedal to the metal in growing online data business while concurrently securing that data. Indeed, the “business” of possessing online data and protecting that data is astronomical. There are seemingly countless incentives for capitalism to remain in the driver seat in light of the billion-dollar per year marketing industry that relies on online data to exist. In the backseat of this vehicle sit the legislators at an all-too-comfortable proximity behind capitalism’s driver. In fact, the legislators enjoy a special privilege amongst all other actors in this vehicle: the ability to steer the entire course of online informational systems and the marketplace in which they thrive. Lastly, sluggishly trailing behind this vehicle is the teardrop camper that houses the judicial system. In a constant state of “catch-up” amongst private businesses and lawmakers, the judicial system is positioned only to witness the vehicle’s actions play out; nothing in its current state permits it to react before calamity strikes.

On June 23, 2016, the United Kingdom (“UK”) voted to leave the European Union (“EU”) in a phenomenon dubbed “Brexit” (British Exit). Due to Brexit, many legal unknowns loom regarding the UK’s future. Broadly speaking, what EU laws will the UK still need to follow? In what areas of law will the UK attempt to distinguish itself from those of the EU? What laws apply to people living in the UK but are citizens of a different EU Member State? Brexit has undeniably triggered these concerns and many more within the UK and in greater Europe.

Partly due to the civil war in Syria, immigration restrictions were once the foundational legal support for a Brexit. Yet there is another area of law, perhaps, that may have influenced the UK’s decision to leave the EU. Leading up to Brexit, another area of law, one with a complicated and controversial past in the EU, went dark on many people’s radar. Recently, however, this area of law has strengthened, which brought with it simultaneous impositions and obligations placed on private companies operating in the EU. With a boundlessly strong future and heavy privatized lobbying regarding implementation, it is no surprise that Internet Privacy is the area of law being described.

Internet Privacy in the EU has been about as smooth of a ride as chasing after the Winnebago Eagle 5 at ludicrous speed.¹ Particularly with the “Right to be Forgotten,” (or the “Right”), the EU experienced polarizing back and forth debates on whether Internet links to information, could be taken down at data-subjects’ requests. The Right empowered data-subjects with a strong Schwartz to demand old, inaccurate, or irrelevant Internet links regarding their lives to be removed.

Internet search engines and data-subjects alike were combing the desert looking for the EU to beam down answers and guidance. Data-subjects finally received fresh air when the EU’s highest court solidified the existence of the Right. With recent EU legislation strengthening online privacy rights, the data-subjects’ radar cleared up in order to combat Internet search engines. Brexit, however, arguably jammed the United Kingdom’s “Right to be Forgotten” radar.

The Right’s implementation is consistently criticized and denigrated by scholars, politicians, and lawmakers alike. While the EU uniformly treats data-subjects as possessing a fundamental right to privacy, the practice of effectuating this right online has been a source of controversy. One prominent opponent of the Right is the UK government.

The “Right to be Forgotten” is an EU doctrine. However, now that the UK is progressing towards leaving the EU in 2019, it is important to examine what jurisprudential changes will follow.² This Comment will examine the “Right to be Forgotten,” the UK’s criticism of the EU Internet doctrine, and the future of the doctrine in the UK once Brexit takes full effect.

The future is somewhat unclear since Brexit arguably jammed the “Right to be Forgotten’s” radar in the UK. Arguments can be made for abandoning the Right and creating a new jurisprudence in the UK. The House of Lords’ commentary fully supports this approach. Yet, the new EU Internet privacy laws, along with accompanying business implications of following these laws, provide other sound reasons for following the EU’s “Right to be Forgotten.” Nevertheless, to Rick Moranis’s delight, it does not appear that Brexit used raspberry jam on the Right’s radar. This Comment concludes that numerous factors weigh in favor of the United

1. Author’s Note: Colonel Sanders, prepare ship for a few Spaceballs references in the Introduction.

2. *UK to exit EU on March 29, 2019 at 11pm*, THE ECONOMIC TIMES (Nov. 10, 2017), <https://economictimes.indiatimes.com/news/international/world-news/uk-to-exit-eu-on-mar-29-2019-at-11-pm-theresa-may/articleshow/61594744.cms>.

Kingdom following the Right's jurisprudence after the country leaves the EU.

Part II of this Comment will discuss the background information of the Right's origin in the EU, culminating in a foundational case and applicable laws that explain precisely what the Right is.

Part III of this Comment will analyze the controversy over implementing the Right in practice, particularly from a UK perspective. It will also explore the frequently perceived negative effects the Right has on businesses and the judicial system.

Part IV of this Comment will consider Brexit's ramifications on the Right, and offers arguments both in favor of adopting the Right and for abandoning it altogether post-Brexit.

Part V of this Comment will attempt to deliver a workable solution to the present-day dilemma of what to do with the Right to be Forgotten and the General Data Protection Regulation ("GDPR"). It will ultimately conclude that the UK should adopt and embrace the Right once it leaves the EU.

II. THE ORIGIN OF THE "RIGHT TO BE FORGOTTEN" IN THE EU

One of Mario Costeja González's last concerns in 1998 regarded the reputational effect his debt and real estate attachment proceedings would have on his life³; yet his story would change the essence of Internet privacy regulations for years to come.⁴ Today, the Right exists in EU Member States due to sixteen years of protracted litigation stemming from Costeja's property ownership.⁵ The interconnectedness of privacy, interpretation, and enforcement of the Right yields a complicated narrative of how this jurisprudential area arose.⁶

3. See Danny Hakim, *Right to Be Forgotten? Not That Easy*, N.Y. TIMES (May 29, 2014), http://www.nytimes.com/2014/05/30/business/international/on-the-internet-the-right-to-forget-vs-the-right-to-know.html?_r=0 ("I was never worried about my online image.") [<https://perma.cc/JD98-33KG>]; Nick Kostov & Sam Schechner, *EU Court to Rule on 'Right to Be Forgotten' Outside Europe*, THE WALL ST. J. (July 19, 2017, 9:56 AM), <https://www.wsj.com/articles/eu-court-to-rule-on-right-to-be-forgotten-outside-europe-1500470225> [<https://perma.cc/ZGK9-9BAJ>].

4. See 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*, 14(4) HUM. RTS. L. REV. 761, 762 (2014), <http://hrlr.oxfordjournals.org/content/14/4/761.short?rss=1&ssource=mfr> [<https://perma.cc/9BBH-4JP4>].

5. See James Ball, *Costeja González and a memorable fight for the 'right to be forgotten'*, THE GUARDIAN (May 14 2014, 11:34 AM), <https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten> [<https://perma.cc/7FX9-GTW8>].

6. See Luciano Floridi, *Should You Have The Right To Be Forgotten On Google? Nationally, Yes. Globally, No.* HUFFINGTON POST (Feb. 25, 2015), <http://www.huffington>

In 2009, the Barcelona newspaper *La Vanguardia* published online some of its archival records that included the decade long story of Costeja's financial problems.⁷ Costeja's debt issues had been rectified and "forgotten" by the time of the online publication, but from the moment of its publication, *La Vanguardia's* story clouded the businessman's reputation.⁸

Costeja acted in response. He requested the newspaper take down the articles relating to him.⁹ When *La Vanguardia* denied his request, Costeja went to Google Spain and requested the news publications be taken down from the Internet.¹⁰ Google Spain originally told Costeja to raise his complaint to its United States' parent company ("Google Inc.").¹¹ Ultimately, Google Spain denied Costeja's request, and thus laid the groundwork for the future sweeping change in Internet privacy law.¹²

Frustrated in his first two attempts to have his past forgotten by the public, Costeja filed suit with the local Agencia Española de Protección de Datos or Spanish Data Protection Agency ("AEPD").¹³ Costeja asked the AEPD for relief against *La Vanguardia*, Google Spain, and Google Inc.¹⁴ The AEPD's opinion found *La Vanguardia* not liable for publishing the news.¹⁵ The AEPD held, however, that Google Spain (and possibly Google Inc.) must "take the necessary measures to withdraw the data from their index and to render access to the data impossible in the future."¹⁶ In essence, the AEPD's decision established Costeja's right to require the Internet

post.com/luciano-floridi/google-right-to-be-forgotten_b_6624626.html [https://perma.cc/5DKT-NZ7S].

7. Miguel Peguera, *The Shaky Ground of the Right to Be Delisted*, 18 VAND. J. ENT. & TECH. L. 507, 523 (2016).

8. *Id.*

9. *Id.*

10. *Id.*

11. Reuters, *The Man Who Sued Google To Be Forgotten*, NEWSWEEK (May 30, 2014, 2:13 PM), <http://www.newsweek.com/man-who-sued-google-be-forgotten-252854> [https://perma.cc/B4C4-SHJ7].

12. *See id.*

13. *Id.*

14. Peguera, *supra* note 7, at 523–24.

15. Court of Justice of the European Union 70/14, Judgment in Case C-131/12 Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez (May 13, 2014), <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> [hereinafter "AEPD Judgment"] [https://perma.cc/4U2P-DLUU].

16. *Id.*

search engine to take down articles regarding his past debts.¹⁷ In narrower terms, however, it appears only data-subjects within the AEPD's territorial jurisdiction could require Internet search engines, such as Google Spain, to remove articles.¹⁸ Yet, the AEDP's decision regarding Google Spain, from a broader perspective, was the first influential domino to fall, paving the way for more powerful courts in this jurisprudential realm.

The EU's General Data Protection Directive 95/46 ("Directive") influenced and controlled the AEPD's decision.¹⁹ For decades, and continuing today, the EU views privacy as an important fundamental right that its citizens possess.²⁰ Adopted in 1995, the Directive solidified the privacy protections of EU citizens "with regard to the processing of personal data and on the free movement of such data."²¹ Within the Directive, there are different thresholds of obligations imposed on private data companies.²² The Directive imposes greater privacy accountability to "controllers" of data, while "processors" have lesser duties.²³ The Directive describes "controllers" of data as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."²⁴ On the other hand, "Processors" of data under the Directive are any "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."²⁵

Controllers bear heavier burdens under the Directive than processors "because they generally decide whether to process data in the first place and then how to do so."²⁶ Controllers under the Directive are required to

17. See Jens-Henrik Jeppsen, *No Right To Be Forgotten says the EU's Advocate General*, CTR. FOR DEMOCRACY & TECH. (June 28, 2013), <https://cdt.org/blog/no-right-to-be-forgotten-says-the-eu's-advocate-general/> [<https://perma.cc/WR3Z-RVN7>].

18. See AEPD Judgment, *supra* note 15.

19. See generally 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 the free movement of such data, 1995 O.J. (L 281), 31, <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476308624577&uri=CELEX:31995L0046> [hereinafter "Directive"] [<https://perma.cc/TWP9-FPK2>].

20. See Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 461–62 (2000).

21. See Directive, *supra* note 19.

22. See Peguera, *supra* note 7, at 520.

23. See *id.*

24. See Directive, *supra* note 19, at art. 2(d).

25. See Directive, *supra* note 19, at art. 2(e).

26. Letter from The Right Honourable Simon Hughes MP, UK Minister of State for Justice and Civil Liberties, to Lord Boswell of Aynho, Chairman of the European Union Committee House of Lords (Oct. 2014), <http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/righttobeforgotten/government-response-right-to-be-forgotten.pdf> [<https://perma.cc/6HEB-6VDR>].

maintain their information as “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.”²⁷ Controllers must also ensure that personal data is accurate and updated regularly.²⁸ Additionally, controllers bear the duty to take “every reasonable step” to erase or rectify incomplete or inaccurate data.²⁹

While the Directive elucidates what controllers and processors of data are, a missing link remained between the AEPD’s decision and how to approach the future issue of takedown requests across the EU. The AEPD held that Google Spain must remove the links relating to Costeja.³⁰ However, the AEPD did not interpret how the language of the Directive applies to Google and Internet search engines moving forward.³¹ Most importantly, whether Google was a data “controller” under the Directive, and thus subject to glaring responsibility, remained unclear following AEPD’s decision.³²

Google Spain and Google Inc. vigorously fought against the AEPD’s decision.³³ Google Spain and Google Inc. wanted to avoid an expensive and drawn out litigation battle with European governments and data protection agencies.³⁴ Google argued it was a passive conveyer of the information on the articles and that merely “linking” the data did not bring the search engine company under the Directive’s umbrella.³⁵ Google asserted *La*

27. See Directive, *supra* note 19, at art. 6(c).

28. See Directive, *supra* note 19, at art. 6(d).

29. *Id.*

30. See Peguera, *supra* note 7, at 525.

31. See *id.*

32. *Id.*

33. See Liam Tung, *Google loses ‘right to be forgotten’ fight in Europe’s top court*, IT IBERIA (May 13, 2014), <http://www.zdnet.com/article/google-loses-right-to-be-forgotten-fight-in-europes-top-court/> [<http://perma.cc/4UGS-JMHL>].

34. See Samuel Gibbs, *Google to extend ‘right to be forgotten’ to all its domains accessed in EU*, THE GUARDIAN (Feb. 11, 2016, 7:40 AM), <https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom> (“Google has been at loggerheads with several EU data protection authorities since the May 2014 ruling by the European Court of Justice”) [<http://perma.cc/V99K-BZJB>].

35. See Craig Newman, *‘A right to be forgotten’ will cost Europe*, THE WASH. POST (May 26, 2014), https://www.washingtonpost.com/opinions/a-right-to-be-forgotten-will-cost-europe/2014/05/26/93bb0e8c-e131-11e3-9743-bb9b59cde7b9_story.html?utm_term=.f8f84759855a [<http://perma.cc/T3D6-JAHD>]; David Meyer, *Google picks holes in EU’s ‘right to be forgotten,’* ZD NET (Feb. 17, 2012, 7:36 AM), <http://www.zdnet.com/article/google-picks-holes-in-eus-right-to-be-forgotten/> [<http://perma.cc/kk2Q3-3JTD>].

Vanguardia was technically the publisher and controller of the information,³⁶ and that extending the Directive to Google would significantly diminish Google’s ability and philosophy to provide a marketplace of ideas.³⁷ Essentially, the Internet search engine company proposed that the Directive did not apply to them because Google did not meet the definition of a “controller.”³⁸

Google appealed the AEPD decision, and the case ultimately reached the Court of Justice of the European Union (“CJEU”).³⁹ The CJEU’s task was to interpret the language of the Directive regarding search engines’ role in privacy.⁴⁰ The CJEU’s landmark decision, commonly known as the *Google Spain* case, held that search engines such as Google are “controllers” of data and the Directive applies.⁴¹

From that moment the “Right to be Forgotten” was officially born. The CJEU determined Google Spain satisfied the requirement of being a “controller” under the Directive because the company “retrieves, records or organizes” data.⁴² “As controllers, search engine operators are obligated to remove links to third party websites containing certain information that identifies an individual by name.”⁴³ The CJEU’s standard is expansive; *Google Spain* calls for data removal if information is “inaccurate, inadequate, irrelevant, or excessive [information] for the purposes of the data processing.”⁴⁴ This standard applies to all Member States within the CJEU’s jurisdiction.⁴⁵

36. See Laura Liguori & Federica De Santis, *The “right to be forgotten”: privacy and online news*, MEDIA LAWS (Mar. 18, 2011), <http://www.medialaws.eu/the-“right-to-be-forgotten”-privacy-and-online-news/> [<http://perma.cc/89RG-EXMK>].

37. See Enrique Chaparro & Julia Powles, *How Google determined our right to be forgotten*, THE GUARDIAN (Feb. 18, 2015), <https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search> [<http://perma.cc/54EA-K9XX>] (“[T]here are all manner of reasons to remove data, other than being compelled by law. One might want to remove information for emotional reasons, ethical reasons, or ‘just because’, when there is no countervailing interest.”).

38. See Recent Case, *Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data Upon Request*, Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 128 HARV. L. REV. 735, 737 (2014).

39. Case C-131/12, Google Spain SL. v. Agencia Espanola de Proteccion de Datos (AEPD), 2014 EUR-Lex 2014 EUR-Lex 62012CJ0131 (May 13, 2014), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN>. [hereinafter “Google Spain”] [<http://perma.cc/64KF-4MVW>].

40. *Id.*

41. *Id.*

42. *Id.*

43. Bunny Sandefur, *The Best Practice of Forgetting*, 30 EMORY INT’L L. REV. 85, 90 (2015).

44. Google Spain, *supra* note 39, ¶ 92.

45. Jeffery Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sept. 29, 2014), <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion> [<http://perma.cc/LZM9-V96H>].

While the new Right was a landmark decision, the rule's name remains somewhat of a misnomer.⁴⁶ The CJEU ruled that Google's links to the articles must be removed, yet the information may still remain accessible to users who do not use search engines.⁴⁷ Some scholars, critics, and commentators have stated the rule is better characterized as the "Right to be Delisted"⁴⁸ or the "Right to Erasure."⁴⁹

Realistically, the CJEU likely contemplated how most people obtain information online and therefore aimed the ruling at search engines' article links. Google controls almost the entire market share for Internet searches;⁵⁰ in turn, the Right is narrowly tailored to links, with regard to search engines' obligations to citizens' privacy interests. The CJEU examined whether "data subject [Costeja] has a right that the information relating to him personally should, at this point in time, no longer be *linked* to his name by a list of results displaying following a search made on the basis of his name."⁵¹ Thus in *Google Spain's* holding, the included "link" language demonstrated the CJEU's legal analysis regarding the current Internet landscape for consuming information.

An important caveat arose from *Google Spain* regarding the CJEU's newly formulated "Right to be Forgotten" rule, namely that the Right is not absolute.⁵² The CJEU in *Google Spain* left open that in some circumstances the Right may not be available to aggrieved plaintiffs,⁵³ such as when there is an "interest of the general public in having access to that information upon a search relating to the data subject's name."⁵⁴ This exception to the Right created a balancing test to determine if the information should remain accessible on the Internet or not.⁵⁵ In *Google*

46. See Peguera, *supra* note 7.

47. *Id.* at 510.

48. *Id.* at 512.

49. See Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433 (2014).

50. Danny Sullivan, *Google Still World's Most Popular Search Engine by Far, But Share of Unique Searchers Dips Slightly*, SEARCH ENGINE LAND (Feb. 11, 2013, 9:00 AM), <http://searchengineland.com/google-worlds-most-popular-search-engine-148089> [<https://perma.cc/7D4U-8T2G>].

51. *Google Spain*, *supra* note 39, ¶ 96 (emphasis added).

52. Court of Justice of the European Union Press Release 70/14, Judgment in Case C-131/12 (May 13, 2014).

53. *Google Spain*, *supra* note 39, ¶ 85.

54. *Id.* ¶ 99.

55. See Sandefur, *supra* note 43, at 90.

Spain, the “balancing of the opposing rights and interests concerned”⁵⁶ pitted the plaintiff’s interest in having information removed from the Internet against the public’s interest in having the information remain available.⁵⁷ As writer James Ball summarized, “the court didn’t establish an absolute right to vanish: ‘a fair balance’ should be sought between the public’s right to access given information and the ‘data subject’s’ right to privacy and data protection.”⁵⁸ The CJEU created a rule that is arguably unconcerned with clarity and bright-line instructions to follow.⁵⁹ Rather, Europe’s highest court set a difficult to predict standard that will ultimately be decided on a case-by-case basis.⁶⁰

Following *Google Spain*, there was substantial uncertainty surrounding the implementation of the CJEU’s Right. The first day following the ruling, Google received more than 12,000 takedown notice requests.⁶¹ Twenty requests per minute made Google and other search engines uneasy about whether compliance with the Right was possible or not.⁶² The “balancing act” of what type of information would be delisted from the Internet on a case-by-case basis made the rule’s practicality dubious at best.⁶³

In the wake of this uncertainty, the Working Party, privacy regulators from the EU’s twenty-eight Member States, met in Brussels on June 3, 2014, to discuss guidelines that data protection authorities in each country would adopt to implement the Right.⁶⁴ Soon thereafter, the Article 29 Working Party (“WP29”) issued guidelines with the purpose of providing a “common ‘tool-box’ to ensure a coordinated approach to the handling of complaints resulting from search engines’ refusals to ‘de-list’ complainants

56. See *Google Spain*, *supra* note 39, ¶ 74.

57. See Sandefur, *supra* note 43, at 90.

58. See James Ball, ‘Right to be forgotten’ ruling creates a quagmire for Google et al, THE GUARDIAN (May 13, 2014, 11:00 AM), <https://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google> [<https://perma.cc/J2C6-C7QG>].

59. Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 371 (2015).

60. See Court of Justice of the European Union Press Release 70/14, *supra* note 52.

61. Sam Schechner, *On Day 1 of European Take-Down Site, Google Hit by Wave of Requests*, WALL ST. J. (May 30, 2014, 3:13 PM), <http://blogs.wsj.com/digits/2014/05/30/on-day-1-of-european-take-down-site-google-hit-by-wave-of-requests/> [<https://perma.cc/>].

62. See *id.*

63. See Chelsea E. Carbone, *To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age*, 22 VA. J. SOC. POL’Y & L. 525, 539 (2015).

64. See *id.*

from their results.”⁶⁵ The WP29 guidelines sought to smooth the Right’s implementation process.⁶⁶ The WP29 attempted to clarify implementation factors such as the connection between the citizen and the online data, whether the citizen is a “public figure,” and the “age” of the online data.⁶⁷

Consequential in the WP29 guidelines was that if a search engine refuses such a takedown request, “the data subject may bring the matter before the Data Protection Agencies (“DPAs”), or the relevant judicial authority, so that they carry out the necessary checks and take a decision in accordance with their power in national law.”⁶⁸ This provision reiterates that citizens and plaintiffs will have judicial recourse available if denied their Right request.

The WP29 guidelines also indirectly support the aforementioned stance that the “Right to be Forgotten” is a misnomer.⁶⁹ The EU took a careful position to protect the citizens only against “links” to harmful information. This position was recapitulated by the WP29 guidelines: “The judgment [*Google Spain*] states that the right only affects the results obtained from searches made on the basis of a person’s name and does not require deletion of the link from the indexes of the search engine altogether.”⁷⁰ Therefore, “the original information will still be accessible using other search terms, or by direct access to the publisher’s original source.”⁷¹

In furtherance of citizens’ privacy rights, the EU replaced the Directive with an updated version of privacy law via the General Data Protection Regulation 2016/679 (“GDPR”) of 2016.⁷² The GDPR will begin applying

65. See Natasha Lomas, *Europe Seeks A Common Appeals Process for the ‘Right to be Forgotten,’* TECHCRUNCH (Sept. 19, 2014), <https://techcrunch.com/2014/09/19/rtbf-appeals-guidelines/> [https://perma.cc/V567-REBB].

66. Article 29 Data Protection Working Party, *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 Costeja González”* C-131/12, at 5, (Nov. 26, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [hereinafter WP29 Guidelines] [https://

67. *Id.* at 13–20.

68. *Id.* at 12.

69. See *id.* at 2.

70. *Id.*

71. *Id.*

72. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) at 1, 2016 O.J. (L 119), <http://eur-lex.europa.eu/>

to EU Member States on May 25, 2018.⁷³ The GDPR strengthens data-subjects' rights with a long list of protections available.⁷⁴ The "Right to be Forgotten" is also strengthened in the GDPR, exemplified from the fact that the process is free to citizens unless the request is "manifestly unfounded or excessive."⁷⁵ The GDPR also places a further burden on the Internet search engines because "the controller [Google for example] should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests."⁷⁶

Under the GDPR, the burden is on search engine companies and other data controllers to prove why the links should remain on the Internet, rather than the citizen to prove the information should be taken down.⁷⁷ Accompanying the Right in the GDPR is an "obligation to take reasonable steps to inform third parties that the data subject has requested erasure of any links to, or copies of, that data."⁷⁸ Support for the GDPR's modernization of privacy laws includes territorial language in the new law: "The right to be forgotten would be an empty shell if EU data protection rules were not to apply to non-European companies and to search engines."⁷⁹ For the first time, the GDPR "leaves no legal doubt that no matter where the physical server of a company processing data is located, non-European companies, when offering services to European consumers, must apply European rules."⁸⁰

Notably, Article 3 of the GDPR pointedly establishes the territorial scope of the new privacy law. Regardless of whether the processing of personal information takes place within the EU or not, "this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union."⁸¹ This language reiterates the territorial reach of the GDPR to companies outside of the EU. As such, Google cannot claim EU privacy laws do not pertain to them as its headquarters are in the United States. Furthermore, when the processing of data relates to goods, services, or monitoring behavior

legal-content/EN/TXT/?uri=uriserv%3AOJ.L_2016.119.01.0001.01.ENG [hereinafter GDPR] [https://perma.cc/ZN8F-A9W8].

73. Memorandum from Allen & Overy LLP on The EU General Data Protection Regulation (2017) at 2, <http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf> [hereinafter "Allen & Overy LLP"] [https://perma.cc/2U6F-TFGH].

74. *Id.* at 7.

75. GDPR, *supra* note 72, at art. 12(5).

76. *See* GDPR, *supra* note 72, ¶ 59.

77. *See generally* GDPR, *supra* note 72.

78. *See* Allen & Overy LLP, *supra* note 73, at 7.

79. *See* Court of Justice of the European Union Press Release 70/14, *supra* note 52.

80. *See id.*

81. *See* GDPR, *supra* note 72, at art. 3.

occurring within the EU, “this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union.”⁸²

The EU, in the form of the 2018 GDPR, builds upon the foundations set forth in the Directive, *Google Spain*, and the WP29 guidelines by imposing enhanced future obligations on data controllers. In examining some of the GDPR’s requirements, Daphne Keller, former legal advisor to Google, criticized the new EU legislation because it could create “a powerful instrument that individuals and companies can use to suppress far more information than GDPR drafters ever intended.”⁸³ The GDPR does streamline a data-subjects’ ability to have links removed from the Internet, but Keller believes the practicality of this system will not solve the issue of voluminous “false accusations made, through ignorance or malice, against legitimate online expression” which Google deals with countless times a day.⁸⁴ Keller believes the online environment for takedown requests is “far too easy for individuals or companies to raise dubious legal claims against content they disagree with, and pressure private Internet platforms to take it down.”⁸⁵ The criticism fixates on the notion that, in regard to the takedown notice requests, adding the pro-data-subjects to the GDPR legislation in 2018 will effectively undercut the protections of lawful expression.

Under the 2018 GDPR, legal advisors such as Keller recommend companies “take user content down immediately upon request, and review the legal allegation later.”⁸⁶ Regardless of whether the content is lawful expression or not, the link to the information is taken down and in most cases “the accused speaker is never told why the online expression disappeared, or given any chance to defend it.”⁸⁷ The protections for lawful expression are subverted in this system because under the GDPR, a “company that gambles on disputing a removal request and leaves challenged content online risks staggering fines—up to €20 million or 4 percent of annual global turnover, whichever is more.” If Keller’s workable concerns are

82. *See id.*

83. Daphne Keller, *The new, worse ‘right to be forgotten,’* POLITICO (Jan. 27, 2016), <http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/> [<https://perma.cc/RR9B-EB2A>].

84. *See id.*

85. *See id.*

86. *See id.*

87. *See id.*

true, then a “remove now and figure it out later” practice will likely manifest resulting in lavish deletion.

III. IMPLEMENTATION OF THE “RIGHT TO BE FORGOTTEN” AND THE UK’S RESPONSE

While the “Right to be Forgotten” is a fundamental EU right supported by *Google Spain* and the GDPR, some practical issues arise concerning the Right’s execution. Bunny Sandefur, writing for the Emory International Law Review, identified three key problems of the Right’s implementation.⁸⁸

Sandefur’s first criticism pertains to the “obstacles and potential privacy vulnerability” EU citizens are exposed to when making a “Right to be Forgotten” request.⁸⁹ Sandefur describes the hoops data-subjects must jump through when making a takedown request. Notably, the obstacles include the incommodious requirement of accessing a computer to make a request, and once a request is made it must be individually transmitted to every respective data-controller of the link.⁹⁰

Some of these barriers Sandefur mentions have been removed by the new GDPR. Data-subjects without an Internet connection could likely not make a request under the old regime, but now most data controllers will have an appointed Data Protection Officer (“DPO”) who receives requests and compliance inquiries.⁹¹ The GDPR further creates a “one-stop-shop” for EU data-subjects to work with, rather than dealing with different local agencies and data controllers.⁹²

In examining the UK’s opposition to the Right’s implementation, Sandefur’s second and third criticisms resound. Sandefur’s second criticism targets *who* is doing the initial balancing determination of “individual privacy, freedom of speech, and public access to information.”⁹³ Under the Right’s policy, Google and other private companies act as the initial “judge and jury in the implementation of personal privacy rights on the Internet.”⁹⁴ Recall that *Google Spain* and the WP29 Guidelines create a “balancing test” when a takedown request is made. At the outset, however, it is not the court determining the fundamental rights of citizens based on particular facts and circumstances. Companies with shareholders, boards of directors, and financial incentives to turn profits conduct the initial “balancing test”

88. Sandefur, *supra* note 43, at 92.

89. *Id.* at 93.

90. *Id.*

91. See Allen & Overy LLP, *supra* note 73, at 3.

92. *Id.* at 6.

93. Sandefur, *supra* note 43, at 102.

94. *Id.* at 103.

of EU citizens' Internet privacy rights.⁹⁵ For example, when an initial request is made to Google, the private company will inform the data-subject: "we [Google] will balance the privacy rights of the individual with the public's interest to know and the right to distribute information."⁹⁶ Moreover, when Google is evaluating a request, Google "will look at whether the results include outdated information about you, as well as whether there's a public interest in the information."⁹⁷

Google has been in conflict with European nations, legislators, and the courts over its "Right to be Forgotten" role since the outset. A driving issue between search engines and Member States is the Right's territorial scope. Google is particularly concerned with EU Member States' insistence that a takedown request of a link in one country should be universally applied.⁹⁸ For example, France fined Google for removing particular links accessible in Europe but not removing the links in the United States.⁹⁹ Google originally fought the Right's scope and territorial reach by claiming a universal delisting would have a chilling effect on the free flow of information.¹⁰⁰ This quandary pitted the United States' First Amendment with the EU's "Right to be Forgotten," but Google eventually found a creative way to satisfy all parties involved.¹⁰¹

Google now uses IP addresses to determine a browser's location when deciding if the previously removed link is viewable or not.¹⁰² For example, "[i]f a German resident successfully requests Google remove a search result under queries for their name, the link will not be visible on any version of Google's website, including Google.com, when the search engine is accessed from Germany."¹⁰³ Nor will the link be visible on any version of Google being accessed by a country subjected to the Right's requirements.

95. EU Privacy Removal, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited Nov. 19, 2016) [<https://perma.cc/CY7B-QUF8>].

96. *See id.*

97. *See id.*

98. *See* Julia Fioretti, *France fines Google over 'right to be forgotten,'* REUTERS (Mar. 24, 2016, 9:38 AM), <http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX> [<https://perma.cc/F78D-U3VQ>].

99. *Id.*

100. *Id.*

101. *See* Samuel Gibbs, *Google to extend 'right to be forgotten' to all its domains accessed in EU,* THE GUARDIAN (Feb. 11, 2016, 7:40 AM), <https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom> [<https://perma.cc/ZDE3-L5Q5>].

102. *Id.*

103. *See id.*

Yet, a United States resident may still be able to access the link if the browsing occurs within the United States. A spokesperson for the French Commission on Information Liberties (“CNIL”) stated the Right’s territorial scope requires “careful thought,”¹⁰⁴ and this compromise by Google regarding the browsers’ IP addresses shows a willingness of the company to comply with its European responsibilities.

From a policy standpoint, it is concerning that private companies are burdened with interpreting the law when that is the reason the judicial system exists. The GDPR attempts to incentivize fairness by imposing substantial fines and “reasonable” obligations for private companies to act in the interest of data-subjects.¹⁰⁵ Under the new GDPR, private companies will need to spend substantial resources on locating *where* the sensitive personal data exists to avoid penalties.¹⁰⁶ Midsized and smaller data companies will conceivably face compliance challenges when the GDPR “audits” begin in 2018.¹⁰⁷ Companies will have a short time to decipher the GDPR’s requirements.¹⁰⁸ Timing concerns also subsist “considering that companies basically will need to implement an enterprise-wide data governance strategy to be able to identify what data exists, where it came from, who has access to it, and why it exists, that’s not much time at all.”¹⁰⁹ The onerous responsibility of private companies conducting “balancing tests” could be undermined by newly created GDPR obligations such as audit compliance. Thus, the practicality of this policy is in doubt.

Sandefur’s third criticism of implementing the Right is the judicial backlog imposed on EU Member States.¹¹⁰ The WP29 guidelines give data-subjects judicial recourse when their takedown notices are denied by controllers after the initial “balancing test.”¹¹¹ DPAs and local courts must now deal with disgruntled data-subjects on appeal after Google determines the information should remain on the Internet.¹¹² The UK was particularly opposed to this backlog effect. Following *Google Spain* and the WP29 guidelines, UK citizens sought to exercise their “Right to be Forgotten” in droves.¹¹³

104. *See id.*

105. *See* Allen & Overy LLP, *supra* note 73.

106. *See* Alex Woodie, *Get a Grip on Your Data Before GDPR Goes Live*, DATANAMI (Oct. 13, 2016), <https://www.datanami.com/2016/10/13/get-a-grip-on-your-data-before-gdpr-goes-live/> [<https://perma.cc/72BK-H96M>].

107. *Id.*

108. *Id.*

109. *See id.*

110. *See* Sandefur, *supra* note 43, at 105.

111. WP29 Guidelines, *supra* note 66, at 12.

112. *Id.*

113. *Thousands of Britons Seek “Right to Be Forgotten,”* BBC NEWS (Oct. 12, 2014), <http://www.bbc.com/news/uk-29586700> [<http://perma.cc/3FRA-6K3M>].

The UK Data Protection Agency tasked with the appeals process is the Information Commissioner's Office ("ICO").¹¹⁴ The ICO maintained that citizens wishing to exercise their "Right to be Forgotten" must first go through the private companies before turning to the ICO.¹¹⁵ Data-subjects cannot seek ICO relief "until the search providers [Google] have had a reasonable time to put their systems in place and start considering requests. After that, [the ICO will] be focusing on concerns linked to clear evidence of damage and distress to individuals."¹¹⁶ The ICO continually stressed concerns regarding the workability of the Right, but the ICO approached this task with the optimism that a fair balance could be struck.¹¹⁷

Whatever minor concerns and resentment the ICO had towards the Right in the EU, the UK's House of Lords expressed a much more hostile disposition toward the doctrine.¹¹⁸ In the House of Lords Committee Report ("Report"), the Lords made it apparent to the world they staunchly opposed the Right.¹¹⁹ The House of Lords and other Parliamentary members describe the CJEU's ruling as "unworkable" and "nonsense."¹²⁰ The Report supports the rule's misnomer characterization and states the rule is better characterized as "the right to make information less easily accessible."¹²¹ The Report criticizes the CJEU for being unrealistic about effectuating the Right: "Once information is lawfully in the public domain it is impossible to compel its removal, and very little can be done to prevent it spreading."¹²² Additionally, the Report suggests the UK did not take issue with the territorial aspect of *Google Spain* and the WP29 Guidelines,¹²³ but instead that the CJEU mischaracterized the language of the Directive.¹²⁴ The House of Lords' Report continually states the CJEU was incorrect in holding the right of erasure

114. See Debbie Heywood, *Google Spain and the 'right to be forgotten,'* GLOBAL DATA HUB (Nov. 2014), https://united-kingdom.taylorwessing.com/globaldatahub/article_2014_google_spain.html [https://perma.cc/85LU-S9NA].

115. *Id.*

116. *Id.*

117. *Id.*

118. See EUROPEAN UNION COMMITTEE, EU DATA PROTECTION LAW: A 'RIGHT TO BE FORGOTTEN?', 2014-15, HL 40 (UK), <http://www.publications.parliament.uk/pa/ld201415/ldselect/lducom/40/40.pdf> [https://perma.cc/74CH-R3Z6].

119. *Id.*

120. See *id.* ¶ 37.

121. See *id.* ¶ 15.

122. See *id.* ¶ 5.

123. See *id.* ¶ 10.

124. See *id.* ¶ 19.

extends beyond “incomplete or inaccurate” data and that Costeja’s information should remain online.¹²⁵

Another goal of the Report is to alleviate some of the Directive’s burdens imposed on Internet search engines.¹²⁶ The House of Lords believes “internet search engine service providers should not be saddled with the obligation of having to assess an unmanageable number of requests on a case by case basis.”¹²⁷ However the House of Lords is not just concerned with Google and other large private companies; “plainly smaller search engines would not necessarily be able to comply with this judgment as easily as Google if they receive a large number of requests.”¹²⁸ The Report chronicles the anxiety surrounding data-subjects’ “uncontested rights of censorship” because smaller search engines would automatically remove links to disputed information given they do not have the resources to examine requests on a case by case basis.¹²⁹

The Report also criticizes the economic impact of the *Google Spain* judgment: “The economic impact on UK businesses of the draft Regulation [GDPR], if enacted in its current form, could be as high as £360 million, of which up to £290 million would be the impact on small and medium enterprises (“SMEs”).”¹³⁰ According to the Report, most UK SMEs are not expected to survive past the start-up phase under the GDPR.¹³¹ While an exact figure could not be given for how much the Right will cost when incorporating the UK judicial system’s involvement, estimates are substantially high.¹³² The House of Lords pleads with the EU that the UK and other Member States “must insist on a text which does away with any right allowing a data subject to remove links to information which is accurate and lawfully available.”¹³³

Parliament Member and Minister of State for Justice Civil Liberties Simon Hughes was also an outspoken adversary to the Right.¹³⁴ Hughes desired the “Right to be Forgotten” to be forgotten in the EU, and stated, “I do not think, both as an individual and a Minister, we want the law to develop in the way that is implied by this judgment, which is that you close down access to information in the EU that is open in the rest of the

125. *Id.*
126. *Id.* ¶ 22.
127. *See id.*
128. *See id.* ¶ 35.
129. *Id.*
130. *Id.* ¶ 43.
131. *Id.*
132. *See id.*
133. *Id.* ¶ 59.
134. *Id.* ¶ 52.

world.”¹³⁵ Hughes made the government’s position clear that the Right should disappear because of the UK’s belief “in freedom of information, and transmission of it.”¹³⁶

IV. BREXIT ANALYSIS AND THE FUTURE IMPACT ON “THE RIGHT TO BE FORGOTTEN” IN THE UNITED KINGDOM

Article 50 of the Treaty on European Union (“TEU”) gives a Member State the right to withdraw from the European Union “either on the basis of a negotiated withdraw agreement or without one.”¹³⁷ The Article 50 process has never been effectuated by a Member State wishing to leave the EU, which means Brexit is a novel situation for the continent.¹³⁸ On March 29, 2017, Prime Minister Theresa May signed a letter on behalf of the UK triggering TEU Article 50. The concern following this triggering of Article 50, however, is whether the process can be halted, and if so by whom.¹³⁹

Prime Minister May’s actions follow from answers to questions concerning the appropriate process behind triggering Article 50. Ever-present were the questions on whether it is the UK Parliament that gives notification to the EU or if it is another branch of the UK government that has the notification power to trigger Article 50.¹⁴⁰

Recently, the High Court in London and the UK Supreme Court addressed this very issue and held that Parliament, and only Parliament, has the authority to trigger Article 50.¹⁴¹ Although the High Court decided the case in early December 2016, the Court waited to announce its ruling until the UK Supreme Court, in a vote of 8-3, affirmed the High Court on

135. *See id.*

136. *See id.* ¶ 53.

137. HOUSE OF COMMONS LIBRARY, BREXIT: SOME LEGAL AND CONSTITUTIONAL ISSUES AND ALTERNATIVES TO EU MEMBERSHIP, 2016, HC 07214, at 4 (UK).

138. *Id.*; Author’s note: this article was written and selected for publication in April of 2017. By the time this article is in fact published in 2018, the United Kingdom undoubtedly will have taken the next steps in effectuating a Brexit. Therefore, this note serves as a reminder the article’s Brexit analysis reflects the environment as of mid-2017.

139. *Brexit: Article 50 has been triggered – what now?*, BBC NEWS (Mar. 29, 2017), <http://www.bbc.com/news/uk-politics-39143978>.

140. *The Article 50 case: Taking back control*, THE ECONOMIST (Nov. 6, 2016), <http://www.economist.com/news/britain/21709589-high-court-rules-parliament-must-vote-trigger-brexit-process-taking-back-control> [<https://perma.cc/9BHA-VCEV>].

141. *Miller v. Sec’y of State for Exiting the EU* [2016] EWHC 2768, Case No. CO/3809/2016 (appeal taken from Eng.), <https://www.judiciary.gov.uk/wp-content/uploads/2016/11/r-miller-v-secretary-of-state-for-exiting-eu-amended-20161122.pdf> [<https://perma.cc/4JML-YFKL>].

January 24, 2017, finding that Parliament must act in order to trigger Article 50.¹⁴² Commentators summarized the High Court’s reasoning: “the 1972 European Communities Act, which gives effect to Britain’s EU membership, is a matter of domestic law, not of foreign policy.”¹⁴³ If the UK wants to reverse the 1972 European Communities Act by triggering TEU Article 50, then the Supreme Court requires Parliamentary action.¹⁴⁴

Interestingly, a “large majority” of current UK Parliament members oppose a Brexit, which may explain why Prime Minister Theresa May and the Executive branch tried to cut Parliament out of the process.¹⁴⁵ The UK Supreme Court’s ruling undoubtedly complicates matters for Prime Minister May.¹⁴⁶ May initially planned an aggressive Brexit triggering process by means of bypassing Parliament through an “ancient crown prerogative power.”¹⁴⁷ Investment manager Gina Miller, wife of hedge-fund manager Alan Miller, brought suit to have the courts interpret Article 50 and its procedural requirements in the UK.¹⁴⁸

Gina Miller, a former London law student, said Prime Minister May’s decision to unilaterally trigger Article 50 “would deny the sovereignty of parliament.”¹⁴⁹ Recently, Miller characterized the argument she and her counsel made to the High Court in London, stating, “once Article 50 is triggered, the legal consequence of the UK withdrawing would inevitably result in citizens’ rights being diminished or removed.”¹⁵⁰ What particularly concerned Miller with Prime Minister May’s plan was “the four freedoms of the free movement of goods, people, services and capital over borders could cease, depending on the exit package the UK government managed to achieve.”¹⁵¹ Fundamentally, Miller’s side advocated that Theresa May could not circumvent the Constitutional principle prescribing Parliament as only having the power to Give and Taketh away citizens’ rights.¹⁵²

142. See *The Article 50 case: Taking back control*, *supra* note 140; see also *Miller v. Sec’y of State for Exiting the EU* [2017] UKSC 5 (appeal taken from Eng.), <https://www.supremecourt.uk/cases/docs/uksc-2016-0196-judgment.pdf> [<https://perma.cc/F7C8-KDMZ>].

143. See *The Article 50 case: Taking back control*, *supra* note 140.

144. *Id.*

145. *Id.*

146. See Richard Allen Greene & Angela Dewan, *Brexit ruling: UK Supreme Court gives parliament Article 50 vote*, CNN (Jan. 24, 2017, 7:39 AM), <http://www.cnn.com/2017/01/24/europe/brexit-article-50-supreme-court-ruling/> [<https://perma.cc/W27K-5KDM>].

147. Gina Miller, *Gina Miller: the Brexit judgment isn’t a victory for me, but for our constitution*, THE GUARDIAN (Jan. 24, 2017, 4:44 AM), <https://www.theguardian.com/commentisfree/2017/jan/24/supreme-court-brexit-judgment-constitution-gina-miller> [<https://perma.cc/UN79-W23C>].

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.*

152. See *id.*

The UK Supreme Court agreed with Miller. Lord David Neuberger read the opinion of the Court and declared “[t]o proceed otherwise [without Parliament] would be a breach of settled constitutional principles stretching back many centuries.”¹⁵³ Seeing Brexit undeniably affects UK citizens’ rights, the UK Supreme Court held that democracy demands those elected by the UK citizens (Parliament) shall be involved in this stage of the Article 50 triggering process.¹⁵⁴ Ironically, and perhaps shifting gears away from democratic rationales, the UK Supreme Court unanimously held in Miller’s case the UK government need not obtain approval of devolved governments in Scotland, Northern Ireland, and Wales to begin the negotiating process.¹⁵⁵

The UK Supreme Court decision means Theresa May cannot start the withdrawal process with the EU until Parliament approves it. May had originally targeted a March 31st deadline to begin unilateral withdrawal without Parliament consent, but now that forecasted date will likely be delayed.¹⁵⁶ Yet, the Executive Branch and May are optimistic that the UK Supreme Court’s ruling will not prolong the withdrawal process long past the March 31st deadline.¹⁵⁷ On January 25, 2017, the day after the UK Supreme Court’s ruling, it was quickly proclaimed that “Theresa May has announced the government will set out its Brexit plans in a formal policy document.”¹⁵⁸ In sum, an Article 50 bill was expected to be published “within days” of the UK Supreme Court’s ruling, but did not attain Royal Assent until March 16, 2017.¹⁵⁹

153. See Green & Dewan, *supra* note 146.

154. See *Brexit: Supreme Court says Parliament must give Article 50 go-ahead*, BBC NEWS: UK POLITICS (Jan. 24, 2017), <http://www.bbc.com/news/uk-politics-38720320> [<https://perma.cc/B5KU-RWBZ>].

155. See *Miller v. Sec’y of State for Exiting the EU* [2017] UKSC 5 (appeal taken from Eng.), <https://www.supremecourt.uk/cases/docs/uksc-2016-0196-judgment.pdf> [<https://perma.cc/F7C8-KDMZ>].

156. See Jen Kirby, *Parliament Has to Make ‘Brexit’ Official, Says the United Kingdom Supreme Court*, THE NEW YORKER (Jan. 24, 2017, 10:02 AM), <http://nymag.com/daily/intelligencer/2017/01/u-k-supreme-court-parliament-has-to-make-brexit-official.html> [<https://perma.cc/HG4T-2HQ2>].

157. See Greene & Dewan, *supra* note 146.

158. See *Brexit: Theresa May promises White Paper on EU exit plan*, BBC NEWS: UK POLITICS (Jan. 25, 2017), <http://www.bbc.com/news/uk-politics-38737967> [<https://perma.cc/M3HD-STBB>].

159. See European Union (Notification of Withdrawal) Act 2017, c. 9 (U.K.), available at http://www.legislation.gov.uk/ukpga/2017/9/pdfs/ukpga_20170009_en.pdf [<https://perma.cc/2JJ6-AGNR>]; Andrew Sparrow, *Brexit: government will introduce article 50 bill ‘within days’ following supreme court ruling – as it happened*, THE GUARDIAN (Jan. 25, 2017, 12:31 PM), <https://www.theguardian.com/politics/blog/live/2017/jan/24/supreme-court->

Now that the UK Supreme Court has decided the procedural process of Article 50, “withdrawal can happen, whether or not there is a withdrawal agreement, two years after the leaving State notifies the European Council of its intention to withdraw.”¹⁶⁰ The European Council sets out the negotiation guidelines for the UK and EU to abide by during the withdrawal process.¹⁶¹ The UK can continually participate in routine business with the EU until the negotiation process is complete.¹⁶² Within the two-year negotiating period, the EU must accede with the UK on “an agreement setting out the arrangements for withdraw and taking into account the ‘framework for [the UK’s] future with the Union.’”¹⁶³

The withdrawal agreements between the UK and EU will likely address momentous issues such as whether the UK will be subject to the jurisdiction of the EU Court of Justice.¹⁶⁴ Also inherent in this withdrawal agreement inquiry will be the future of the “Right to be Forgotten.” While it is not clear whether the Right will be incorporated into the negotiated withdrawal agreements between the UK and EU, it is clear the “withdrawal agreement will have to be implemented by an Act, or Acts, of Parliament.”¹⁶⁵

The UK Parliament is composed of two houses: the House of Commons and the House of Lords.¹⁶⁶ The House of Lords has adamantly reiterated their rancorous stance on the Right,¹⁶⁷ so it is foreseeable that when the House of Lords participates in enacting the withdrawal agreement there may be lobbying for change in this specific area of Internet Privacy. Although the House of Lords cannot exclusively block a Brexit from happening, it may be able to delay the process and express their strong opinions to the other parties involved about what issues that must be agreed upon when leaving the EU. As of April 2017, no explicit word has come from the House of Lords regarding the Right’s future post-Brexit.

Once the UK leaves the EU, “many individual rights are likely to be covered in a withdrawal agreement negotiated under Article 50 TEU.”¹⁶⁸ If the future of the “Right to be Forgotten” is not negotiated in the withdrawal agreement between the UK and EU, could the Right be construed as an

article-50-judgement-announces-its-article-50-judgment-politics-live [<https://perma.cc/7HYT-KT6V>].

160. See HOUSE OF COMMONS LIBRARY, *supra* note 137, at 6.

161. *Id.*

162. *Id.*

163. *See id.*

164. *Id.* at 8.

165. *Id.* at 9.

166. *The two-House system*, UK PARLIAMENT, <http://www.parliament.uk/about/how/role/system/> (last visited Sept. 29, 2017) [<https://perma.cc/P2LR-S952>].

167. See EUROPEAN UNION COMMITTEE, *supra* note 118.

168. HOUSE OF COMMONS LIBRARY, *supra* note 137, at 19.

“Acquired Right”? Proponents who want the Right to exist in the UK post-Brexit would argue yes.

Acquired Rights, also known as “vested,” “executed,” or “conferred” rights, would continue to provide certain EU protections to UK citizens if the country leaves the Union without an agreement.¹⁶⁹ Giving a particular individual “protection” is the essence of an “Acquired Right,”¹⁷⁰ “[f]or all [its] imprecision, the term has been adopted by usage.”¹⁷¹

Another principle supporting the Acquired Rights doctrine is the concern over legislative retroactivity operating to thwart individual liberties.¹⁷² When significant change occurs in a country, the doctrine of Acquired Rights steps in to protect the ex post facto unraveling of established important values created under the old regime.¹⁷³ French Legal Philosopher Antoine Pillet summarized the doctrine in the following manner: “[E]very time a right has been regularly acquired in any country, the right must be respected and its effects must be guaranteed to it in another country belonging.”¹⁷⁴ This principle is illustrated in Scotland’s Supreme Civil Court holding, which stated, “the purpose of the acquired rights directive was to ensure that the rights of employees were safeguarded in the event of a change of employer.”¹⁷⁵

Two characteristics must generally be satisfied to be considered an Acquired Right: (1) it must be a part of the estate of a specific person acquired in a regular and proper manner; and (2) it must be concrete and of a private nature.¹⁷⁶ Furthermore, “if a right has both private and public aspects, it can only be an acquired right where the private aspects predominate.”¹⁷⁷

It is clear the “Right to be Forgotten” has both private and public aspects when making an Acquired Rights determination. Typically, under a privacy rationale, one seeks to have private content removed from the public

169. See Case C-60/98, *Butterfly Music Srl v. Carosello Edizioni Musicali e Discografiche Srl*, 1999 EC.R. 1-3957 (discussing acquired rights to third parties).

170. Pierre A. Lalive, *The Doctrine of Acquired Rights*, in *RIGHTS AND DUTIES OF PRIVATE INVESTORS ABROAD* 145, 150 (Mathew Bender ed., 1965).

171. *Id.* at 151.

172. *Id.* at 153.

173. See *id.* at 154.

174. *Id.* at 157–58.

175. *Meechan v. Sec’y of State for Scot.*, (1996) 1997 S.L.T. 936, 939 (Scot.) (quoting *Foreningen Arbejdskedere I Danmark v. Daddy’s Dance Hall A/S*, 1988 E.C.R. 752).

176. Robert B. von Mehren, 76 AM. J. INT’L L. 909 (1982) (reviewing JACQUES BARDE, *LA NOTION DE DROITS ACQUIS EN DROIT INTERNATIONAL PUBLIC* (1981)).

177. See *id.*

domain. However, it seems reasonable to understand this umbrella of Internet “Privacy” as considerably more private than public.

With regards to the UK, there are certain statutorily recognized employee rights meeting the definition of “Acquired Rights.”¹⁷⁸ Directive 2001/23 protects the “rights of employees in the event of the transfer into new ownership of the business in which they are employed.”¹⁷⁹ Primarily the protections extend to “transfers of a business [where] employees of that business are transferred with it.”¹⁸⁰ For example, Acquired Rights would attach when “the employees’ contract of employment with A undergoes a statutory novation and becomes a contract of employment with B.”¹⁸¹ In sum, the Acquired Rights of employees under the statute are protected from “potentially detrimental consequences resulting from a transfer of the undertaking in which they are employed.”¹⁸²

Measures have been made to protect employee rights in the event of a significant transfer. This rationale could be applied to protecting data-subject’s privacy rights in the event of a significant transfer out of the EU. Furthermore, the free movement of goods and workers are considered Acquired Rights, hence there is the possibility that the “free movement of data”¹⁸³ could be interpreted as an Acquired Right. As previously described, the free movement of people, or prevention thereof, was a significant reason for Brexit’s initial popularity. The UK would have to make a distinction if it chooses to stand by its position on limiting immigration and at the same time allowing the free movement of data in a post-Brexit landscape. The UK would also face criticism in characterizing the “Right to be Forgotten” as an Acquired Right.

One way to distinguish the free movement of people from the free movement of data is the tangible and physical presence of a person compared to cyber data. Due to the modern trends in hacking and Internet database breaches, modern societies understand how harmful free access to unsecured data can be. In this regard, the UK will need to make a policy decision covering whether it is more important to secure its borders against tangible people, digital data, both, or neither when the country decides the terms of their withdrawal agreement. Nevertheless, Acquired Rights typically deal with international treaties, which do not shed light on the particularized case law and EU legislation-born Right.

178. FRANCIS BEAUFORT PALMER ET AL., *PALMER’S COMPANY LAW*, ch. 14, 14.148 (25th ed., Mar. 2015).

179. *See id.*

180. *See id.*

181. *See id.*

182. *See id.*

183. *See generally* GDPR, *supra* note 72.

A different argument also suggests the view that EU case law creates Acquired Rights for individuals. In 1963, the CJEU held in *van Gend & Loos* that “EU law confers rights on the nationals of the Member States that become part of their ‘legal heritage.’”¹⁸⁴ EU rights enforceable in any national court are likely considered “Acquired” under this definition because rights formulated under an individual’s legal heritage should outlast the mechanism that created it.¹⁸⁵

Following significant change and legislation in a country, two exceptions exist for a “right” to fall outside the doctrine of Acquired Rights. First, subsequent legislation divulging certain liberties could be justified under a public policy rationale.¹⁸⁶ Second, if “the right acquired abroad corresponds to no right known and organized in the local law” of the new regime, then it is likely not an Acquired Right.¹⁸⁷ The UK’s local data protection laws incorporate the EU’s old Directive 95/46;¹⁸⁸ therefore, post-Brexit legislative change regarding the “Right to be Forgotten” could be arguably justified under a public policy approach because of the impracticality of the EU rule.

In the event that this area of Internet Privacy is not negotiated in UK withdrawal agreements, whether or not the Right is an Acquired Right has significant implications on data-subjects living in the UK. Post-Brexit, EU law would no longer apply in the UK. This means, “not only would the EU treaties cease to apply, but any national law implementing EU law would have to be repealed, amended, or possibly retained.”¹⁸⁹ The House of Lords reckoned the concept of determining Acquired Rights would be “one of the most complex aspects” of the UK’s withdrawal negotiations.¹⁹⁰ Would the Right be a part of the UK citizens’ legal heritage to retain the “fundamental” right of erasing links? Or would public policy dictate the UK’s justification in departing from the EU’s unworkable jurisprudence?

184. See HOUSE OF COMMONS LIBRARY, *supra* note 137, at 20.

185. *Id.*

186. See Lalive, *supra* note 170, at 158.

187. *See id.*

188. See Nathalie Moreno, *The Implications of Brexit for UK Data Protection law*, LEWIS SILKIN LLP INSIGHTS (July 21, 2016), <http://www.lewissilkinemployment.com/en-gb/insights-knowledge/insights-knowledge/a/insights/implications-brexit-uk-data-protection-law/> [https://perma.cc/Y4TZ-R7XR].

189. See Sionaidh Douglas-Scott, *What Happens to ‘Acquired Rights’ in the Event of a Brexit?*, UK CONST. L. ASS’N BLOG (May 16, 2016), <https://ukconstitutionallaw.org/2016/05/16/sionaidh-douglas-scott-what-happens-to-acquired-rights-in-the-event-of-a-brexit/> [https://perma.cc/8ZVM-5X7W].

190. House of Lords Select Committee on the European Union, *The Process of Withdrawing from the European Union*, HL 138 ¶ 26, May 4, 2016.

The House of Lords recently examined the Acquired Rights Brexit issue and declared “the doctrine of acquired rights in international law is limited both in scope and enforceability, and is highly unlikely to provide meaningful protection against the loss of EU rights upon Brexit.”¹⁹¹ The Lords further provided insight into how they suggest dealing with Acquired Rights by stating “the rights to be safeguarded in the withdrawal agreement should be frozen as at the date of Brexit.”¹⁹² The idea behind this policy is to create a “level playing field” in which “the parallel EU rights evolve over time, so it is likely that UK law will have to evolve with them.”¹⁹³ By creating a system in which “UK law can take account of relevant developments in EU law, and, importantly, that EU law can take account of relevant developments in UK law,”¹⁹⁴ the Lords seem to suggest continued incorporation of the UK with EU law post-Brexit.

The bulk of the Lords’ recent Acquired Rights report dealt with citizenship rights, but the policy and principles published by the Lords can provide discernment into how the country will balance EU interaction with independent UK efforts in autonomy. What is clear in the Lords’ recent report is that jurisprudential “developments” will be accounted for and recognized post-Brexit. The Right’s future, however, is unclear, in that UK developments might or might not influence change in Internet privacy and EU developments might or might not dictate the UK’s jurisprudence.

More likely to happen, however, is that the Right’s future will be included in the Brexit withdrawal negotiations. Negotiating data privacy positions will be imperative for the UK withdrawal agreements due to the importance of UK businesses being able to “share data freely between establishments based in the EU and the UK.”¹⁹⁵ The UK will be in position to decide from three likely “Models” regarding Internet Privacy in a post-Brexit regime: The Norwegian Model, the Swiss Model, or the “Do it Alone” Model.¹⁹⁶

The concept of a single data market would be the driving factor for the UK to decide to follow the Norwegian Model.¹⁹⁷ Yet, the Norwegian

191. See EUROPEAN UNION COMMITTEE, BREXIT: ACQUIRED RIGHTS, REPORT 10, 2016-17, HL 82, at 3 (UK), <http://www.publications.parliament.uk/pa/ld201617/ldselect/ldeucom/82/82.pdf> [<https://perma.cc/E2VZ-NA77>].

192. See *id.*

193. See *id.*

194. See *id.* at 4.

195. *Brexit: Impact on Data Privacy and Cybersecurity*, GREENBERGTRAUIG LLP (July 25, 2016), <http://www.gtlaw.com/News-Events/Publications/Alerts/196732/Brexit-Impact-on-Data-Privacy-and-Cybersecurity>.

196. See *id.* The Norwegian Model, the Swiss Model, or the “Do it Alone” Model will be discussed in detail *infra* this section.

197. See *id.*

Model would only be possible if the UK joined the European Free Trade Association (“EFTA”) and the European Economic Area (“EEA”).¹⁹⁸ The EEA, of which all EU Member States as well as Norway, Iceland, and Liechtenstein are members, gives “substantial” access to the EU single market and free movement of “goods, services, people and capital.”¹⁹⁹ Moreover, the Norwegian Model would “preserve the status quo on *data flow* between the UK and other EEA Member States.”²⁰⁰

However, there are also reasons why the UK may be hesitant to follow the Norwegian Model in a post-Brexit regime. As mentioned, the Norwegian Model requires EEA Member States to accept free movement of people.²⁰¹ This requirement may not coincide with the UK’s stance of immigration reform supporting Brexit.²⁰² Further, the Norwegian Model requires EEA Member States to make financial contributions to the EU.²⁰³ Yet an underlying component supporting Brexit was the UK’s vexation over its financially disproportionate contributions to the EU.²⁰⁴ For years, tensions escalated between the UK and EU over financial contributions,²⁰⁵ so it is unlikely the UK will choose a model where they are required once again to pay into the EU. Lastly, under the Norwegian Model, “the UK would have to implement data privacy laws that are [harmonized] with EU law (in other words, the GDPR).”²⁰⁶ The House of Lord’s unease with the GDPR’s strengthened Right counts against the UK affirmatively adopting the Norwegian Model.

198. *See id.*

199. HOUSE OF COMMONS LIBRARY, *supra* note 137, at 28.

200. *See Brexit: Impact on Data Privacy and Cybersecurity*, *supra* note 195.

201. HOUSE OF COMMONS LIBRARY, *supra* note 137, at 28.

202. Peter Walker, *Brexit: Theresa May prioritises immigration curbs over single market*, THE GUARDIAN (Oct. 2, 2016, 11:54 AM), <https://www.theguardian.com/politics/2016/oct/02/brexit-theresa-may-prioritises-immigration-curbs-over-free-movement> [<https://perma.cc/9X65-ZJWB>].

203. HOUSE OF COMMONS LIBRARY, *supra* note 137, at 28.

204. Alice Foster, *Brexit: When will Britain STOP paying billions into the EU budget at long last?*, SUNDAY EXPRESS (Sept. 29, 2016, 3:55 PM), <http://www.express.co.uk/news/politics/715849/Brexit-when-Britain-stop-paying-billions-EU-budget-financial-contributions-UK-payments> [<https://perma.cc/V8DJ-4E69>].

205. John Stevens, *Britain is punished for outpacing Europe as contributions to Brussels leap by £3.1 billion over the next five years*, DAILYMAIL.COM (July 9, 2015), <http://www.dailymail.co.uk/news/article-3154628/Britain-punished-outpacing-Europe-contributions-Brussels-leap-3-1-billion-five-years.html>.

206. *See Brexit: Impact on Data Privacy and Cybersecurity*, *supra* note 195.

Under the Swiss Model, the UK would “seek confirmation from the European Commission that its data privacy laws are ‘adequate’ to protect personal data.”²⁰⁷ Switzerland is a member of the ETFA but not the EU. To gain limited access to the single market, Switzerland has negotiated over 100 separate agreements with the EU.²⁰⁸ Separate negotiations and contracts with the EU could be the foundation of the UK’s decision to pick the Swiss Model. If the “UK were to obtain adequacy status, it would join the EU’s ‘white list’ of adequate countries.”²⁰⁹ Thus, under the Swiss Model, the UK could enact its own version of the GDPR to satisfy “adequacy” status. Presumably, if the UK were to choose this model, Parliament may try and maneuver a GDPR compliant statute while chipping away at the Right’s unworkable characteristics. Nevertheless, based on the type of separate agreement with the EU, the Swiss Model does require certain financial contributions and immigration flow.²¹⁰ These potential obligations may deter the UK from choosing the Swiss Model. Furthermore, the UK government has already hinted that the Swiss Model might be an impractical choice.²¹¹ Securing numerous separate agreements with the EU, just as Switzerland did, would be “unlikely” for the UK.²¹² The EU-Swiss separate agreements were described by the UK government as “complicated, and increasingly controversial both with the EU and in Switzerland.”²¹³ The UK recognizes that “both the EU and the Swiss are calling the viability of this model into question,”²¹⁴ which likely weighs in favor of the UK not choosing this model.

A third, but unlikely, option exists in the UK deciding to follow the “Do it Alone” Model.²¹⁵ Under the “Do it Alone” Model, the UK could “develop its own data protection legislation without regard to EU law,”²¹⁶ but efforts to significantly distance the UK away from the GDPR could result in negotiating incommensurable business mechanisms between UK and EU data companies. The territorial reaches of the new GDPR would require UK data companies under the “Do it Alone” Model to go to great lengths “to permit the lawful transfer of data from the sites and servers of their

207. *See id.*

208. HOUSE OF COMMONS LIBRARY, *supra* note 137, at 30.

209. *See Brexit: Impact on Data Privacy and Cybersecurity*, *supra* note 195.

210. HOUSE OF COMMONS LIBRARY, *supra* note 137, at 30.

211. HM Government, *Alternatives to membership: possible models for the United Kingdom outside the European Union*, ¶ 3.43 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504604/Alternatives_to_membership_-_possible_models_for_the_UK_outside_the_EU.pdf [<https://perma.cc/ETX7-VGCZ>].

212. *Id.*

213. *See id.*

214. *See id.*

215. *See Brexit: Impact on Data Privacy and Cybersecurity*, *supra* note 195, at 3.

216. *See id.*

customers . . . located in the EEA to those servers of the UK business that are located in the UK.”²¹⁷ Businesses in the UK seeking to work with other Member States would have to comply with the territorial reach of the EU’s GDPR. This makes the “Do it Alone” Model a complicated endeavor.

Compliance could conceivably occur through separate contracts or trade agreements, but if the UK tries to develop its own model of Internet privacy, and the offered UK protections don’t satisfy the GDPR’s requirements, the country risks a business hiatus with GDPR countries. Additionally, the “Do it Alone” Model imposes significant burdens on data companies operating in the UK to comply with the already significant burdens of the GDPR, and for this reason this Model seems to be an implausible option.

In this context, the UK has an important post-Brexit decision to make in choosing what to do with the Right. However, even though the UK hinted against it, the Swiss Model is likely the best option. The UK may try a path where compliance with the GDPR is satisfied regarding free flow of data, while also formulating a more practical way regarding implementation of the Right. This raises an important question of whether the UK can alter the “Right to be Forgotten’s” jurisprudence while still abiding and remaining “adequate” by the GDPR.

Commentators for the Privacy and Data Protection group acknowledge that “despite Britain’s vote to leave the EU, UK organisations will face a data protection and cyber security law landscape heavily influenced by EU laws for the foreseeable future.”²¹⁸ The ICO in further supporting the GDPR’s influence in the UK recognizes that “once implemented in the EU, the GDPR will be relevant for many organisations in the UK—most obviously those operating internationally.”²¹⁹ Anya Proops, writing for the Privacy and Data Protection Group, also believes that due to the timing of the Article 50 exit process, it is “highly likely that the GDPR will become law in the UK prior to any effective Brexit.”²²⁰

Proops suggests the UK’s Internet privacy situation post-Brexit is analogous to Hotel California: “the UK can check out any time it likes, but in terms

217. *Id.*

218. *There’s no getting around it: New UK law will be closely aligned with GDPR*, PRIVACY & DATA PROTECTION J., July-Aug. 2016, at 1.

219. *See id.*

220. Anya Proops, *Brexit and the future of data protection*, PRIVACY & DATA PROTECTION J., July-Aug. 2016, at 8.

of data protection, it can never altogether leave.”²²¹ Proops’s accurate simile pertains to the key substantive points of protecting data under the GDPR, such as breach notification and data portability.²²² Does the Right qualify as a key substantive component of the GDPR? Proops hints the Right may still need to be followed because “if we [the UK] want to maintain our adequacy status, those rules will still have to ensure that data subjects enjoy effective remedies in respect of breaches of their data protection rights.”²²³ Achieving adequacy status under the Swiss Model without giving the effective remedy of erasing links in the UK could pose a speed bump in a post-Brexit jurisdiction.

The reason for the GDPR’s influence in the UK post-Brexit is because of Article III’s aforementioned territorial reach: “Article [III] of the GDPR requires that non-EU states afford an equivalent level of legal protection as that required under EU law.”²²⁴ In other words, the GDPR applies “when personal data of EU citizens is processed by entities outside the European Union ‘regardless of whether the processing takes place in the Union or not,’ so long as such entities have an establishment within the European Union.”²²⁵ The territorial reach of the GDPR’s Article III presents enormous commercial implications for UK businesses. Due to these implications, the ICO Commissioner expects UK businesses to “comply with standards equivalent to those under the GDPR to enable them to transfer data around the EU for business purposes” in the future.²²⁶ Failure to comply with the GDPR, even post-Brexit, will result in “substantial fines . . . imposed by data protection regulatory authorities across the EU upon a UK company.”²²⁷

Thus, the UK will have a daunting decision to make when withdrawal negotiations materialize: adopt the “Right to be Forgotten” to protect UK businesses operating under the GDPR, enact its own “adequate” version of the GDPR while also constricting the Right’s future in the UK, or abandon the Right altogether.

221. *See id.*

222. *See There’s no getting around it: New UK law will be closely aligned with GDPR*, *supra* note 218, at 17.

223. *See* Proops, *supra* note 220, at 9.

224. Hugh J. McCarthy, *Decoding the Encryption Debate: Why Legislating to restrict strong encryption will not resolve the “Going Dark” problem*, *J. INTERNET L.*, Sept. 2016, at 1, 34.

225. *Id.*

226. Adam Hartley, *Brexit: 10 Steps for Employers to Take Now*, *DLA PIPER BE AWARE UK* (July 7, 2016), <http://www.dlapiperbeaware.co.uk/b-rexit-10-steps-for-employers-to-take-now-2/> [<https://perma.cc/HJK7-7L5E>].

227. *See* James Mullock, *Brexit—a data protection perspective*, *PRIVACY & DATA PROTECTION J.*, June 2016, at 14–15.

V. WHY THE UNITED KINGDOM WILL CONTINUE TO FOLLOW THE
“RIGHT TO BE FORGOTTEN” POST-BREXIT

There are many compelling reasons to believe the UK will want to diverge from the Right.²²⁸ The UK may try and maneuver an “adequate” compliance with the GDPR while also abandoning the Right. Moreover, the UK could adopt the GDPR while implementing a different version of the Right. Perhaps the UK will adopt a version of the Right that is practical and workable to the House of Lords’ liking. Nevertheless, because the GDPR will already be in place by the time Brexit is effectuated²²⁹ and the financial consequences of not complying with the GDPR are significant, the United Kingdom will likely abide by the Right.

The UK government’s main responsibility is to do what is best for its citizens and economy. In this regard, maintaining business relations with the EU will be imperative for stability and creating a unique identity post-Brexit. In a digital global economy, it would be far too risky to subject Internet companies located in the UK to a situation where they cannot trade or source cyber information with EU Internet companies. With the respect to the Right, the best decision the UK can make for economic prosperity purposes is to follow the GDPR. In sum, with regards to adequate GDPR compliance: if you cannot fit, you must submit.

228. *See supra* Part III.

229. *See supra* Part IV.

