AN OCEAN APART: THE TRANSATLANTIC DATA PRIVACY DIVIDE AND THE RIGHT TO ERASURE

PAUL J. WATANABE*

TABLE OF CONTENTS

* J.D., University of Southern California Gould School of Law, 2017. The author thanks Sam Erman for his sage advice and the editors of *Southern California Law Review* for their diligence and camaraderie.

INTRODUCTION

Cindy Lee Garcia faced multiple death threats.[1] Garcia was cast in a bit role in a short film—a thriller set in ancient Arabia. She spoke a couple of lines, appeared on screen for about five seconds, and earned five hundred dollars—not a bad gig.[2] Unfortunately for her, the final product was not quite what she thought it would be.[3] *Innocence of Muslims*, "an anti-Islam polemic" that "depicts the Prophet Mohammed as, among other things, a murderer, pedophile, and homosexual," featured Garcia's performance; her lines were dubbed over "with a voice asking, 'Is your Mohammed a child molester?'"[4] The video garnered millions of views on YouTube, and Garcia's participation in the production, despite her inability to control the final product, saw her life threatened.[5] Garcia asked Google to remove the video from YouTube, but Google declined to do so.[6] After a court battle, Garcia was ultimately unsuccessful in getting the video taken down from YouTube.[7]

Mario Costeja González felt that Google was treading on his dignity.[8] In 1998, a newspaper published a notice that Costeja González's real property would be auctioned because he had failed to pay off social security debts.[9] Although he could not get the article removed from the newspaper's website, Costeja González wanted Google to remove the article—a dozen years after its publication—from search results for his name.[10] He contended that the search results were unfair because the debt proceedings against him had been resolved for years, "and that reference to

1. Garcia v. Google, Inc., 786 F.3d 733, 737 (9th Cir. 2015) (en banc).
2. *See id.*
3. *See id.* at 736.
4. *Id.* at 737.
5. *Id.* at 736–38.
6. *Id.* at 738.
7. *Id.* at 747.
8. Ashifa Kassam, *Spain's Everyday Internet Warrior Who Cut Free from Google's Tentacles*, GUARDIAN (May 13, 2014, 1:24 PM), http://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez.
9. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, EU:C:2014:317 ¶ 14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN.
10. *Id.* ¶¶ 14–15.

them was now entirely irrelevant."[11] Ultimately, Costeja González successfully got the article removed from search results for his name.[12]

What separates Garcia's plight from Costeja González's are the figurative ocean currents of data privacy values diverging over time, as well as the literal ocean dividing the United States and the European Union. The Ninth Circuit summarized the transatlantic divide in *Garcia v. Google, Inc.*:

> Privacy laws . . . may offer remedies tailored to Garcia's personal and reputational harms. . . . Ultimately, Garcia would like to have her connection to the film forgotten and stripped from YouTube. Unfortunately for Garcia, such a "right to be forgotten," although recently affirmed by the Court of Justice for the European Union, is not recognized in the United States.[13]

The case that affirmed the "right to be forgotten" was Costeja González's—*Google Spain SL v. Agencia Española de Protección de Datos*.[14] The right recognized by the high court of the European Union in *Google Spain* allowed users to demand from Google the delisting or removal of their personal information.[15] Not only did this right require Google, a private Internet company, to respond to individuals' requests to be forgotten, but it also required other intermediaries—companies running search engines and other Internet services that handle personal data[16]—to "forget" information that was "inadequate, irrelevant or no longer relevant, or excessive."[17] Intermediaries had to adapt quickly to their new responsibility to safeguard a European right[18] that was but an aspiration of data privacy reformists before the European high court divined it from a nearly twenty-year-old nonbinding directive.[19] *Google Spain* marked a

11. *Id.* ¶ 15.

12. *Id.* ¶ 98.

13. Garcia v. Google, Inc., 786 F.3d 733, 745 (9th Cir. 2015) (en banc) (citations omitted).

14. European Court of Justice Press Release No. 70/14, An Internet Search Engine Operator is Responsible for the Processing That It Carries Out of Personal Data Which Appear on Web Pages Published by Third Parties (May 13, 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

15. *See, e.g.*, THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN, FINAL REPORT 3–4 (2015) [hereinafter ADVISORY COUNCIL], https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf.

16. Daphne Keller, *Intermediary Liability and User Content Under Europe's New Data Protection Law*, CTR. FOR INTERNET & SOC'Y STAN. L. SCH: BLOG (Oct. 8, 2015, 6:00 AM), http://cyberlaw.stanford.edu/blog/2015/10/intermediary-liability-and-user-content-under-europe's-new-data-protection-law.

17. *Google Spain*, EU:C:2014:317 ¶ 94.

18. *See, e.g.*, ADVISORY COUNCIL, *supra* note 15, at 4–6.

19. *See* European Commission Press Release IP/12/46, Commission Proposes a Comprehensive

notable clash between the United States and the European Union's different data privacy regimes, as EU users could assert the right to be forgotten across the Atlantic, requiring U.S. private and public entities to weigh European privacy values.[20]

More concretely, the case was decided against the backdrop of a sea change in Internet privacy reforms at the EU level. Two years before the decision in *Google Spain*, the European Commission promulgated a so-called right to be forgotten in the draft text for a regulation to replace the aging Data Protection Directive ("DPD" or "Directive"), modernizing data protection rules and harmonizing them among the European Union's member states.[21] After years of negotiation,[22] this new, comprehensive, self-executing law, the General Data Protection Regulation ("GDPR" or "Regulation"), will take effect in May 2018.[23] Building upon the groundwork laid by *Google Spain*, the GDPR contains a "[r]ight to erasure" that codifies and expands the right to be forgotten online.[24] With the GDPR, the European Union is poised to swiftly and completely reconstruct the legal pillars of European data protection.[25]

On the other side of the Atlantic, the United States approaches data protection from a different perspective. The U.S. government faces political gridlock on domestic data privacy reform,[26] while existing privacy rights are limited to specific sectors and weighed against First Amendment

Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012) [hereinafter European Commission Press Release IP/12/46], http://europa.eu/rapid/press-release_IP-12-46_en.htm.

20. *See infra* Part II.

21. European Commission Press Release IP/12/46, *supra* note 19.

22. *See* European Commission Statement 15/5257, Remarks by Commissioner Jourová After the Launch of the Data Protection Regulation Trilogue (June 24, 2015), http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm. The trilogue concluded in December 2015, and the text adopted at the conclusion of the trilogue is considered to be substantively finalized. Cedric Burton et al., *The Final European Union General Data Protection Regulation*, BNA (Feb. 12, 2016), http://www.bna.com/final-european-union-n57982067329.

23. *See* Parliament & Council Regulation 2016/679, art. 99, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

24. *Id.* art. 17.

25. *See* European Commission Press Release IP/16/216, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm; Daphne Keller, *New EU Law Will Tell U.S. What Can Be Said—and Built—on the Internet*, RECODE (Oct. 14, 2015, 6:00 AM), http://recode.net/2015/10/14/new-eu-law-will-tell-u-s-what-can-be-said-and-built-on-the-internet; *infra* Parts II & III.

26. Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES (Feb. 27, 2015), http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html.

free speech concerns.[27] With unanswered concerns regarding the revelation of foreign surveillance programs conducted by the National Security Agency, as well as the perceived inadequacy of the United States' protection of individuals' privacy rights,[28] the European Union has taken a comparatively more protective, omnibus approach to data privacy reform.[29]

The incongruity of U.S. and EU data protection regimes derives from the European Union's recognition and prioritization of privacy as a fundamental right.[30] Whereas the U.S. Constitution does not provide any facial guarantees of privacy,[31] the right of privacy is enshrined in a number of foundational EU documents—including the European Convention on Human Rights[32] and the Charter of Fundamental Rights of the European Union[33]—as well as the landmark Directive that the GDPR replaces.[34] Rights prioritization across the Atlantic is a study of contrast: the United States favors free expression over privacy, and the European Union balances privacy and free expression as coequal fundamental rights.[35] Unsurprisingly, U.S. and EU data privacy values diverged because of this foundational disconnect between European and American values, manifesting in conflicting data protection schemes.[36] The potentially broad impact of the GDPR challenges the coexistence of disparate privacy regimes, as the Regulation's provisions may serve as a tool for the European Union to export its data privacy values.[37]

27. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 143–44, 790–91 (5th ed. 2015).

28. *See, e.g.*, Case C-362/14, Schrems v. Data Prot. Comm'r, EU:C:2015:650 ¶¶ 28–31, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en.

29. *See* GDPR, *supra* note 23, recital 104; European Commission Press Release IP/12/46, *supra* note 19.

30. *See* Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 416 (2015); *infra* Part I.

31. *See* Lawrence Siry, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, 103 KY. L.J. 311, 329 (2014–2015).

32. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter Convention].

33. Charter of Fundamental Rights of the European Union, arts. 7–8, 2010 O.J. (C 83) 389, [hereinafter Charter].

34. Parliament & Council Directive 95/46, art. 1, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive]. As discussed *infra* in Part III.A, the Data Protection Directive will be superseded by the GDPR. GDPR, *supra* note 23, art. 94.

35. *See* JEANNE PIA MIFSUD BONNICI, SELF-REGULATION IN CYBERSPACE 62 (Aernot H.J. Schmidt et al. eds., 2008).

36. *See id.* at 122; Siry, *supra* note 31, at 343; *infra* Part I.

37. *See* Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 194 (2012) ("Inaction, however, is not an option as the conflict has already manifested itself in the tensions that exist between the approach to regulation taken in the European Union and the approach taken in the United States."). *See infra* Parts II & III.A.

The *Google Spain* right to be forgotten and the GDPR right to erasure emblemize the imminent threat to the coexistence of the two data protection regimes.[38] The right recognized by the European Court of Justice in *Google Spain*[39] sees U.S.-based "data controllers"—a term that initially encompassed only intermediaries like search engines,[40] but under the GDPR will include many other entities[41]—removing or delinking "inadequate, irrelevant or no longer relevant, or excessive" information upon request by a European data subject.[42] Data controllers apply a balancing test to decide whether personal information must be erased, weighing the "interest of the general public in having . . . access to the information" with the interest of the data subject.[43] The GDPR takes the right to another level, obligating "the controller . . . to erase personal data without undue delay,"[44] providing narrow exceptions, including an exception, "to the extent that processing is necessary," "for exercising the right of freedom of expression and information."[45]

Matters get complicated when U.S.-based data controllers subject to the new European regulation are tasked with adjudicating the erasure right. First, data controllers are required to weigh free expression and privacy rights coequally, which contrasts with the familiar prioritization of free expression in the United States.[46] Second, although the GDPR harmonizes data protection laws across the European Union, freedom of expression and information laws remain fractured at the state level; the Regulation cursorily tasks member states to reconcile their free expression laws with the GDPR.[47]

Because of these complications, U.S. data controllers must act as courts of first instance and apply fractured expression laws against a

38. This Note uses "right to erasure" to denote the right delineated in the GDPR and "right to be forgotten" to denote the right recognized by the European Court of Justice in *Google Spain*.

39. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, EU:C:2014:317 ¶ 99, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN.

40. Keller, *supra* note 16.

41. *See* GDPR, *supra* note 23, art. 4(7); Keller, *supra* note 16.

42. *Google Spain*, EU:C:2014:317 ¶ 94. Data subjects must be "natural persons" to request erasure. *See* Directive, *supra* note 34, art. 1(1).

43. *Google Spain*, EU:C:2014:317 ¶ 99.

44. GDPR, *supra* note 23, art. 17(1).

45. *Id.* art. 17(3).

46. Bennett, *supra* note 37, at 164–65; Rustad & Kulevska, *supra* note 30, at 354. *See* MIFSUD BONNICI, *supra* note 35, at 62; *infra* Part II.A.

47. *See* GDPR, *supra* note 23, art. 85. Likewise, under the *Google Spain* right to be forgotten, data controllers had to apply the law of the member state in which the person requesting to be forgotten resides. *See Google Spain*, EU:C:2014:317 ¶ 9 (quoting Directive, *supra* note 34, art. 9).

supposedly harmonized European data protection regime.[48] If the implementation of the *Google Spain* right to be forgotten, which required data controllers to apply the law of the member state in which the person exercising the right to be forgotten resides,[49] is any indication, adjudication of the right to erasure could get messy quickly. Under *Google Spain*, a US intermediary had to evaluate a French citizen's delisting request under French freedom of expression laws and under the purview of the data protection rules set forth by the French data protection authority, whereas the same intermediary had to evaluate an Irish citizen's identical request to be forgotten under Irish freedom of expression laws and under the purview of the Irish authority.[50]

As a result, the free expression side of the adjudicative scale remains fractured at the national level, obscuring the privacy-expression balance that U.S. companies must adjudicate. Modifying the previous example, under the GDPR, Google must implement delisting decisions based on the new pan-European data protection rules, but the company still may be required to weigh data protection interests against the disparate national freedom of expression laws of France or Ireland.[51]

Despite the variance of freedom of expression laws among European member states, the Regulation endeavors to allay the problems of implementing privacy rights by harmonizing data protection rules and centralizing authority over those rules in a European Data Protection Board.[52] But continued fragmentation of free expression principles across member states, and new principles introduced in the GDPR that encourage forum-shopping create an opportunity for U.S. data controllers to ignore the European Union's attempt to export its privacy values across the Atlantic.[53] Perspicacious data controllers can choose lead supervisory authorities from nations with favorable views toward national free expression laws, putting a finger on the expression side of the scale.[54]

48. *See* Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017, 1023–25 (2016); *infra* Part II.B.

49. *See* Rustad & Kulevska, *supra* note 30, at 359.

50. *See* 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, ¶ 16 (2014) [hereinafter Working Party Implementation Guidelines], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

51. *See* GDPR, *supra* note 23, arts. 17, 85. *See infra* Part III.B.

52. GDPR, *supra* note 23, arts. 68, 70. *See infra* Part III.C.

53. *See infra* Part III.

54. *See infra* Parts III.B & III.C.

Though U.S. data controllers are subject to the new EU privacy regime, unharmonized freedom of expression laws among EU member states provide a powerful tool that may undermine the effectiveness of the new data protection regime.[55]

This Note argues that fragmented free expression laws across European member states and data controllers' ability to select their reviewing supervisory authority give U.S. data controllers latitude to exploit the privacy-expression balance in favor of the U.S. prioritization of expression. Whereas the current literature revolving around the right to be forgotten and the GDPR focuses on reconciling and converging transatlantic values of privacy and free expression, this Note examines the mechanisms of the European Union's assertion and imposition of privacy values across the Atlantic through the right to be forgotten and the right to erasure and describes weaknesses in the GDPR that may undermine those mechanisms.

Part I outlines the diverging paths that led to the rift in data protection policy. Part II details how the experimental implementation of the *Google Spain* right to be forgotten preliminarily exported the European privacy scheme across the Atlantic, previewing the potential impact of the GDPR's right to erasure. Part III outlines the provisions of the GDPR that thwart the right to be forgotten as a tool of imposing EU privacy values on U.S. data controllers. The Conclusion prophesies the ultimate effects of the Regulation on American privacy values, given the Regulation's flaws.

I. DIVERGENT PRIVACY PRIORITIZATIONS LED TO CONFLICTS IN DATA PROTECTION SCHEMES

The United States and the European Union have vastly different valuations of privacy. Whereas the European Union's guiding principles enshrine the right to privacy as a fundamental right,[56] the United States' penumbral protections of privacy subordinate the interest to others, like free expression,[57] the most notable countervailing right at stake in critiques of the *Google Spain* right to be forgotten.[58]

55. *See infra* Conclusion.

56. *See infra* Part I.A.

57. *See infra* Part I.B.

58. *See, e.g.*, Francoise Gilbert, *Symposium Review: European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 847 (2011-2012) (citing Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012), www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten).

A. THE EUROPEAN UNION ENSHRINES PRIVACY AND DATA PROTECTION AS FUNDAMENTAL HUMAN RIGHTS COEQUAL WITH THE FREEDOM OF EXPRESSION AND INFORMATION

The European Union recognizes a fundamental human right in its foundational sources of individual rights policy guidance. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights, recognizes a person's "right to respect for his private and family life, his home and his correspondence."[59] Though "[t]he European Convention is an instrument created by the Council of Europe," which includes the EU member states as well as a number of other countries,[60] the high court of the European Union acknowledged that Article 8 of the Convention "constitutes part of basic legal principles of the European Union."[61]

Article 7 of the Charter of Fundamental Rights of the European Union, which became legally binding after the Treaty of Lisbon took force in 2009, declares that "[e]veryone has the right to respect for his or her private and family life, home and communications."[62] Article 8 then identifies a separate, "'third generation' fundamental right[]" to data protection:[63] "Everyone has the right to the protection of personal data concerning him or her."[64] The Charter specifies that individuals have the right to access collected data and "the right to have it rectified."[65]

But the fundamental nature of the privacy right does not mean that the right is unchecked. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms lists exceptions in which the privacy right may be inhibited, most pertinently "for the protection of the rights and freedoms of others."[66] Although the Charter of Fundamental Rights does not contain similar exceptions in the privacy and data protection articles, the EU treats the various rights identified in the Charter as equal and subject to "the principle of proportionality"[67] in determining which right

59. Convention, *supra* note 32, art. 8(1).

60. Ronald J. Krotoszynski, Jr., *Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis*, 56 WM. & MARY L. REV. 1279, 1283–84 (2015).

61. *Id.* at 1284–85 n.13 (citing Case C-62/90, Comm'n v. Fed. Republic of Ger., 1992 E.C.R. I-2575, I-2609).

62. Charter, *supra* note 33, art. 7.

63. *EU Charter of Fundamental Rights*, EUROPEAN COMMISSION: JUSTICE, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (last visited Aug. 14, 2017).

64. Charter, *supra* note 33, art. 8(1).

65. *Id.* art. 8(2).

66. Convention, *supra* note 32, art. 8(2).

67. Charter, *supra* note 33, art. 52(1).

prevails in the case of a conflict.[68] Thus, when coequal rights conflict, "no clear interpretive guidance exists on the hierarchy of rights."[69]

Of relevance here, the right to freedom of expression and information also is elevated to the status of a fundamental right in the European Union. The Council of Europe included the freedom of expression as a fundamental right in Article 10 of the Convention,[70] which is repeated almost verbatim in Article 11 of the European Union's Charter.[71] Given the principle of proportionality espoused by the Charter, adjudicators must weigh the right of privacy and the right of free expression and information "on a case-by-case basis."[72] Not infrequently, the privacy right prevails over the freedom of expression and information.[73]

Since its promulgation in 1995, the European Union's Data Protection Directive has provided adjudicators somewhat more guidance in adjudicating privacy-expression conflicts as it sought to better harmonize European member state laws regarding data protection. Although the Directive was proposed and adopted well before the modern Internet and the rise of "big data" companies,[74] it has been the guiding force on data protection policy for the past twenty years.[75] It provides additional, stronger privacy protections than member states had enacted, and it rejects "the laissez-faire mentality" in privacy protection.[76]

Specifically, the DPD was designed to ensure that "Member States . . . protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[77] For example, the DPD provides that natural persons can request personal information collected from them or about them;[78] access

68. Patricia Sánchez Abril & Jacqueline D. Lipton, *The Right to Be Forgotten: Who Decides What the World Forgets?*, 103 KY. L.J. 363, 372 (2014–2015) (citing Charter, *supra* note 33, art. 52).

69. *Id.*

70. Convention, *supra* note 32, art. 10(1) ("Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."). *See* Siry, *supra* note 31, at 319 (citing Joined Cases C-465/00, C-138/01 & C-139/01, Rechnungshof v. Österreichischer Rundfunk, 2003 E.C.R. I-5014, I-5042).

71. Charter, *supra* note 33, art. 11(1).

72. Abril & Lipton, *supra* note 68, at 372.

73. Rustad & Kulevska, *supra* note 30, at 357–58.

74. Recent Case, *Case C-131/12*, Google Spain SL v. Agencia Española de Protección de Datos, *(May 13, 2014)*, 128 HARV. L. REV. 735, 735 (2014).

75. *See* Rustad & Kulevska, *supra* note 30, at 359.

76. ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY 3 (2008).

77. Directive, *supra* note 34, art. 1(1).

78. *Id.* arts. 10–11.

collected data and rectify, erase, or block improperly processed data;[79] and object to processing of their personal data,[80] among other rights.[81]

But the DPD restates rather than resolves the problem of how to balance privacy and expression.[82] It requires member states to provide "exemptions or derogations" for journalistic, artistic, or literary expression "only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[83]

Despite its aspiration to bring about a "coherent data protection regime,"[84] the Directive left a patchwork of data protection rules in its wake. As a nonbinding directive, the DPD only sets implementation goals for member states to meet through national laws.[85] It was not a regulation directly binding on member states.[86] Therefore, member states used the Directive as guidance in creating or modifying national legislation, "which resulted in divergent data protection rules in different EU countries."[87] Thus, member states implemented dozens of individual national laws.[88] Member states apply the DPD and its privacy rights in different ways, including in their weighing of the free expression and information derogations.[89] The Directive required each member state to set up a supervisory authority—also referred to as a data protection authority[90]—to monitor implementation of national personal data processing rules and to hear claims regarding them.[91] National—as opposed to pan-European—implementation led to further fragmentation. According to the European Commission's Impact Assessment Board, DPD "exemptions in relation to

79. *Id.* art. 12. Article 12(b), which plays an important part in *Google Spain*, requires member states to guarantee that data subjects have the right to obtain from the controller "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data." *Id.* art. 12(b).

80. *Id.* art. 14. Article 14(a), which is also instrumental in *Google Spain*, grants data subjects the right "to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation." *Id.* art. 14(a).

81. *See generally id.* ch. II.

82. *See id.*, pmbl. ¶ 37.

83. *Id.* art. 9.

84. Directive, *supra* note 34, pmbl. ¶ 7; Siry, *supra* note 31, at 317–18.

85. Gilbert, *supra* note 58, at 824; *Regulations, Directives and Other Acts*, EUROPEAN UNION, https://europa.eu/european-union/eu-law/legal-acts_en (last visited Aug. 14, 2017).

86. Gilbert, *supra* note 58, at 824.

87. Rustad & Kulevska, *supra* note 30, at 359.

88. Gilbert, *supra* note 58, at 817.

89. *Commission Staff Working Paper, Impact Assessment*, annex 2, at 22–23, SEC (2012) 72 final (Jan. 25, 2012) [hereinafter *Impact Assessment*].

90. *See* European Commission Press Release IP/12/46, *supra* note 19.

91. Directive, *supra* note 34, art. 28.

freedom of expression create increasing uncertainty . . . . [T]he application of data protection rules for disclosing to the public information, opinions or ideas, in relation to the freedom of expression should be clarified."[92]

Even though the right to privacy is fundamental in the European Union, the right is checked by other fundamental rights, including the right to freedom of expression and information. Particularly in the context of data protection, the often-countervailing rights are weighed in disparate ways among the member states. Yet as fractured as the EU approach remains, it is recognizably more protective of privacy than U.S. law.

B. THE UNITED STATES HAS WEAKER PRIVACY RIGHTS AND PRIORITIZES FREE EXPRESSION OVER PRIVACY

Unlike the express protections of privacy in the European Union, the U.S. Constitution contains no express guarantee of privacy.[93] Instead, the American notion of the right to privacy traces its theoretical origins to an 1890 *Harvard Law Review* article penned by Samuel D. Warren and Louis D. Brandeis:[94]

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." . . . [N]umerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[95]

Warren and Brandeis envisioned a right of privacy as a necessary response to technological innovation causing the private to become public.[96] Though Warren and Brandeis were concerned with "[i]nstantaneous photographs and newspaper enterprise" creating a gossip trade,[97] the sentiment that technological progress engenders privacy issues echoes in the modern context of data protection.[98] Yet Warren and Brandeis's solution to the privacy problem sounded in tort, not in constitutional values; privacy still had an uncertain status as a

92. *Impact Assessment*, *supra* note 89, at 23.

93. *See* Siry, *supra* note 31, at 329 (citing Griswold v. Connecticut, 381 U.S. 479, 483–85 (1965)).

94. *See* JONATHAN I. EZOR, PRIVACY AND DATA PROTECTION IN BUSINESS: LAWS & PRACTICES 1 (2012).

95. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890).

96. *Id.*

97. *Id.*

98. EZOR, *supra* note 94, at 4.

constitutional right.[99]

Since the Warren and Brandeis article, the Supreme Court of the United States has recognized a right to privacy emanating from provisions in the Bill of Rights.[100] "[P]enumbras" of privacy give substance to the guarantees laid out in the Bill of Rights, including the First Amendment.[101] The Court has recognized that there may be a privacy interest in "avoiding disclosure of personal matters"[102] and in "keeping personal facts away from the public eye."[103] But this penumbral right to privacy in the U.S. Constitution is far more limited than the right recognized by the European Union. The Bill of Rights insulates individuals from only government interference with privacy.[104] Some states have embraced the Warren and Brandeis conception of invasion of privacy as a series of torts that can be brought against a private entity, but privacy torts are not uniformly recognized in the United States.[105]

There is no "comprehensive privacy framework" for personal data in the United States.[106] Instead, self-regulation among data market participants reigns supreme.[107] Stemming from concerns that over-regulation would impede development and innovation in a growing market, the United States historically has been wary to interfere with data markets by imposing privacy regulations.[108] As opposed to the positive, rights-based European approach to data privacy regulation, the United States views data privacy as an economic or commercial matter, as the "processing of personal data constitutes quite a considerable part of the entire market sector."[109]

Because individual privacy protections against private actors are not

99. *See* Warren & Brandeis, *supra* note 95, at 211.

100. EZOR, *supra* note 94, at 2.

101. Griswold v. Connecticut, 381 U.S. 479, 483–84 (1965).

102. Whalen v. Roe, 429 U.S. 589, 599 (1977).

103. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 769 (1989).

104. Siry, *supra* note 31, at 329.

105. *See* SOLOVE & SCHWARTZ, *supra* note 27, at 33; William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (describing four types of privacy invasions often recognized at common law); Siry, *supra* note 31, at 329 (citing MARY MCTHOMAS, THE DUAL SYSTEM OF PRIVACY RIGHTS IN THE UNITED STATES 21 (Robert M. Howard ed., 2013).

106. Rustad & Kulevska, *supra* note 30, at 377.

107. *See* JOANNA KULESZA, INTERNATIONAL INTERNET LAW 60 (Magdalena Arent & Wojciech Woloszyk trans., 2012); MIFSUD BONNICI, *supra* note 35, at 19; SOLOVE & SCHWARTZ, *supra* note 27, at 791.

108. KULESZA, *supra* note 107, at 58.

109. *Id.*

uniform across the United States, and because the private self-regulatory regime is perceived as adequate for addressing privacy issues, state and federal governments have been slow to regulate data markets to protect individual privacy; government actors do not want to kill the goose that lays the golden eggs, so they trust that private companies' self-regulation adequately protects privacy.[110] As a result, privacy protections in the United States are reduced to "a patchwork of legislation, regulation, and self-regulation."[111]

Recently, some efforts have been made to upend the current self-regulatory scheme in favor of stronger affirmative privacy protections for Internet users. The Obama administration introduced the Consumer Privacy Bill of Rights in 2012, which aimed to give Americans "the right to control personal information about themselves" with "strong" enforcement by the Federal Trade Commission.[112] The Consumer Privacy Bill of Rights aimed to improve global Internet interoperability with "mutual recognition of privacy frameworks . . . and enforcement cooperation."[113] But the text of the administration's proposed bill was not released until early 2015,[114] and the draft was promptly criticized by both the European Data Protection Supervisor and the Federal Trade Commission Chairwoman for its ineffectiveness.[115] The bill is not likely to make headway in the sitting Republican-controlled Congress.[116]

The most aggressive U.S. regimes of data protection arise at the state level, though all remain far less protective of the data privacy right than the European Union. The state leader in the area is California,[117] which in 2015 enacted a statute that requires data companies to permit minors "to remove or . . . to request and obtain removal of, content or information

110. *See* MIFSUD BONNICI, *supra* note 35, at 19.

111. Rustad & Kulevska, *supra* note 30, at 376.

112. Office of the Press Sec'y, *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights*, WHITE HOUSE (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

113. *Id.*

114. THE WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

115. Allison Grande, *FTC, EU Officials Say Privacy Bill of Rights Lacks Bite*, LAW360 (Mar. 5, 2015, 9:16 PM), http://www.law360.com/articles/628365/ftc-eu-officials-say-privacy-bill-of-rights-lacks-bite.

116. Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES (Feb. 27, 2015), http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html.

117. *See* SOLOVE & SCHWARTZ, *supra* note 27, at 793–94.

posted . . . by the user."[118] The right is a narrow one, however; only minors benefit, and those minors may seek erasure only of content they themselves created.[119] Although California's stricter privacy laws often set the standard that private entities follow for all U.S. states,[120] state legislators' influence is limited at present given the general national preference against regulating data protection[121] and the lack of uniform national laws protecting privacy.[122]

Contrasting with the nebulous protections of privacy, the right to free expression and information is well-defined in the United States. The right of free speech traces its origins to the inception of the nation, "born of dissent and distrust of government institutions,"[123] and the expression right often takes prevalence over other rights.[124] The First Amendment prohibits Congress from "abridging the freedom of speech, or of the press."[125] Accordingly, privacy interests derived from the tort common law must be weighed against the potential for abridgment of free speech through that common law.[126] The Supreme Court has interpreted the free speech right expansively, often favoring free speech over libel, defamation, and other tort claims that have privacy implications.[127] Thus, when privacy and free speech conflict, the concrete constitutional right to free speech is often favored over the more nebulous protections of privacy.[128]

Given the dominance of the right of free speech, it is no wonder that countervailing privacy rights are underdeveloped in the United States' data

118. CAL. BUS. & PROF. CODE § 22581(a)(1) (West 2016). State legislators in Illinois and New Jersey are working to adopt a similar minor data protection law. Caitlin Dewey, *How the 'Right to be Forgotten' Could Take Over the American Internet, Too*, WASH. POST (Aug. 4, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/08/04/how-the-right-to-be-forgotten-could-take-over-the-american-internet-too.

119. CAL. BUS. & PROF. CODE § 22581(a)(1); Rustad & Kulevska, *supra* note 30, at 380.

120. SOLOVE & SCHWARTZ, *supra* note 27, at 793.

121. MIFSUD BONNICI, *supra* note 35, at 19.

122. Siry, *supra* note 31, at 329.

123. Laura R. Palmer, *A Very Clear and Present Danger: Hate Speech, Media Reform, and Post-Conflict Democratization in Kosovo*, 26 YALE J. INT'L L. 179, 205 (2001).

124. UTA KOHL, JURISDICTION AND THE INTERNET 108 (2007).

125. U.S. CONST. amend. I.

126. SOLOVE & SCHWARTZ, *supra* note 27, at 144 ("Although the privacy torts are litigated by private parties, they employ the machinery of the state (its tort law and legal system) to impose costs on" private parties.).

127. *See* Krotoszynski, *supra* note 60, at 1282–83 (noting "the one-sided, speech-favoring outcomes of the *New York Times Co. v. Sullivan*, *Hustler Magazine, Inc. v. Falwell*, and *Snyder v. Phelps* line of cases").

128. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1106–10 (2000).

privacy regime.[129] With the First Amendment trumping privacy concerns, comprehensive privacy reforms withering on the vine, and self-regulation dominating the data protection sphere, the United States is not likely to enforce or sustain stringent data protection regulations. The United States does not value the privacy right at the same level as the right to freedom of expression and information. Thus, divergence between the United States and the European Union's systems of data privacy protections was inevitable.

II. *GOOGLE SPAIN* PROTOTYPED THE RIGHT TO BE FORGOTTEN AND EXPORTED EUROPEAN DATA PRIVACY PRIORITIZATION

With the rampant growth of the border-defying Internet, the contrasting privacy regimes came to a head as U.S.-based companies wrangled with the European Union's data protection rules.[130] The United States and the European Union reached an agreement that permitted U.S. companies to self-certify that they would comply with the data privacy values outlined in the DPD, facilitating a satisfactory yet uneasy détente.[131] American companies could process American user data under the domestic scheme of self-regulation,[132] and they could deal in European user data by following European rules abroad.[133]

But the détente was fleeting. The initial proposal for the GDPR, a self-executing pan-European privacy regulation aiming to update and replace the DPD, was issued in January 2012,[134] and it had a domino effect on the transatlantic data privacy relationship. The highest court of the European Union, the Court of Justice, issued a number of pivotal decisions in the mid-2010s that endorsed the sweeping, extraterritorial scope of the draft Regulation's privacy protections and dismissed the American data privacy

129. *See* Rustad & Kulevska, *supra* note 30, at 379.

130. *See id.* at 386.

131. Commission Decision, annex 1, 2000 O.J. (L 215) 7 (EC). This détente experienced some tumult in 2015, when it was invalidated due to Edward Snowden's revelations of the U.S. National Security Agency's access to personal data of European citizens controlled by companies subject to the agreement. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, EU:C:2015:650 ¶ 105, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en. The Privacy Shield, which replaced the original Safe Harbor Agreement, provides stronger protections against U.S. government interference, yet maintains the concept of private organizations' self-certifying their compliance with EU law. European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.htm.

132. *See supra* notes 107–10.

133. Bennett, *supra* note 37, at 174–75.

134. European Commission Press Release IP/12/46, *supra* note 19.

regime as inadequate.[135] In *Google Spain*, the Court of Justice divined a right to be forgotten, first put forth in the January 2012 Regulation draft, from the nearly twenty-year-old DPD, implementing a novel system of rights-balancing that requires private American companies to adjudicate European data protection values.[136] *Google Spain*'s implications question the propriety of maintaining divergent data privacy regimes and test the exportation of European data privacy values across the Atlantic by requiring American companies to adopt the European regime even domestically.

A. THE *GOOGLE SPAIN* DECISION DERIVED A RIGHT TO BE FORGOTTEN FROM THE DATA PROTECTION DIRECTIVE

The right to be forgotten recognized in *Google Spain* demonstrates the tensions that arise when European privacy protections are imposed upon U.S. companies operating in a very different privacy regime. In *Google Spain*, a man requested that Google Spain "remove or conceal" from Google search results for his name a true but "entirely irrelevant" newspaper announcement involving attachment proceedings against him.[137] The Spanish data protection authority upheld the complaint under the DPD, "consider[ing] that [the] obligation [to withdraw or prohibit access to data] may be owed directly by operators of search engines."[138] The case wound its way to the EU Court of Justice, which agreed with the Spanish authority and proclaimed that search engines such as Google fell under the Directive's definition of "data controllers."[139] This meant that search engine companies were subject to additional obligations to ensure data protection and privacy.[140]

The Court of Justice confirmed that the DPD can apply to data controllers even when their data processing activities occur entirely outside the territory of a member state. A data controller is subjected to the national data protection laws of a member state in which it is "established."[141] Even if its processing of personal data took place entirely outside EU territory,

135. *See* Abigail Slater, *The Tremor, Quake, and Aftershock of EU Privacy Norms*, REG. REV. (Feb. 2, 2016), https://www.theregreview.org/2016/02/02/slater-eu-privacy-norms-us.

136. See *infra* Part II.A.

137. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, EU:C:2014:317 ¶ 14–15, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN.

138. *Id.* ¶ 17.

139. *Id.* ¶ 38.

140. Krotoszynski, *supra* note 60, at 1328.

141. Directive, *supra* note 34, art. 4(1)(a).

Google was within the reach of the DPD solely because it carries out "the promotion and sale of advertising space" in Spain.[142]

The Court of Justice then articulated that the DPD established a "right to be forgotten," which obliges a search engine operator to remove search results "in order to comply with the rights laid down in" Articles 12(b) and 14(a) of the Directive.[143] Upon the exercise of this right, search engines are required to remove search results that are "inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes [for which data were collected or processed] and in the light of the time that has elapsed," even if that information is truthful.[144] But making the decision whether to remove results requires balancing countervailing rights and interests.[145] Refusing the request may be "justified by the *preponderant* interest of the general public in having . . . access to the information in question."[146] Nevertheless, privacy and data protection "rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information."[147]

Notably, the search engine operator is the adjudicating entity in the first instance of the erasure decision.[148] Though the Court of Justice's decision indicates that erasure requests should be granted in the default case,[149] it entrusts the data controller to ensure that the Directive's guarantees are met.[150] Thus, *Google Spain* practically "place[s] a burden on many global, information-processing businesses to implement procedures to protect individual personal data . . . . with little to no governmental or judicial oversight."[151]

142. *Google Spain*, EU:C:2014:317 ¶¶ 46, 48.

143. *Id.* ¶ 88. Google's Advisory Council on the Right to Be Forgotten suggests that the ruling "does not establish a general Right to be Forgotten," but instead a narrower right to request delisting from search query results. ADVISORY COUNCIL, *supra* note 15, at 3–4. Nevertheless, this Note uses the term "right to be forgotten" in the context of *Google Spain* because of the right's similarity to the right proposed in the GDPR and because the delisting right is popularly referred to by that name.

144. *Google Spain*, EU:C:2014:317 ¶ 93.

145. *Id.* ¶ 74.

146. *Id.* ¶ 99 (emphasis added).

147. *Id. Accord* Abril & Lipton, *supra* note 68, at 372 ("Spanish courts have often capitulated to privacy interests where they determine that time has made the noxious information irrelevant (or, in American legal terminology, not of legitimate public concern) or outdated.").

148. *See Google Spain*, EU:C:2014:317 ¶¶ 83–84; Abril & Lipton, *supra* note 68, at 380. The Article 29 Data Protection Working Party indicated that the *Google Spain* decision may apply to other types of Internet intermediaries. *See* Working Party Implementation Guidelines, *supra* note 50, ¶ 17.

149. *See Google Spain*, EU:C:2014:317 ¶ 99.

150. *Id.* ¶ 83.

151. Abril & Lipton, *supra* note 68, at 366; *accord* Lee, *supra* note 48, at 1066.

This put data controllers like Google in a bind. Private data controllers located outside the European Union[152] can be subjected to European data privacy laws,[153] which means they are required to remove content upon request unless they employ a test of unfamiliar but fundamental European rights.[154] This test proportionately balances privacy and data protection against freedom of expression and information,[155] but it eschews the economic interests of the data controllers.[156] And all of this occurs in a nascent area of law with shallow precedents from European authorities and courts. Private, often foreign entities serve as adjudicators of first instance.[157]

Needless to say, initial reactions to *Google Spain* from legal critics were largely negative.[158] Notably, the European Union Committee of the British House of Lords found *Google Spain* "unworkable,"[159] stating that "[i]t is wrong in principle" to permit search engines to adjudicate delisting decisions.[160] The European Union Committee recommended resisting entirely the inclusion of a right to be forgotten or a right to erasure in the GDPR.[161]

Even though the Court of Justice found authority in the DPD for the right to be forgotten, the Directive itself does not explicitly grant that right or suggest that data controllers should engage in interest-balancing.[162]

152. *See* Rustad & Kulevska, *supra* note 30, at 362 ("European countries have often imposed regulations on the Internet that have extraterritorial effects on U.S. companies.").

153. Directive, *supra* note 34, art. 4(1)(a); *Google Spain*, EU:C:2014:317 ¶¶ 46, 48.

154. *See Google Spain*, EU:C:2014:317 ¶ 99.

155. Abril & Lipton, *supra* note 68, at 371–72 (citing Charter, *supra* note 33, art. 52). *Cf. supra* Part I.A.

156. *Google Spain*, EU:C:2014:317 ¶ 81.

157. *See* Abril & Lipton, *supra* note 68, at 366 ("[W]hile businesses are socially and practically unfit to become the ultimate arbiters of privacy, they may now have been effectively thrust into that unenviable position.").

158. *See* Recent Case, *supra* note 74, at 738–39.

159. EUROPEAN UNION COMMITTEE, EU DATA PROTECTION LAW: A 'RIGHT TO BE FORGOTTEN'?, 2014-5, HL 40, ¶ 56 (UK), http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf.

160. *Id.*

161. *Id.* ¶ 65.

162. *See* Directive, *supra* note 34, art. 12(b) (guaranteeing the "rectification, erasure or blocking of data . . . in particular because of the *incomplete or inaccurate nature* of the data" (emphasis added)); *id.* art. 14(a) (granting the right "to object at any time on compelling legitimate grounds . . . to the processing of data relating to him"). Note that the Article 12(b) guarantee relates to incomplete or inaccurate data—a far cry from the true but irrelevant data considered in *Google Spain*. Curiously, a version of the right to be forgotten was expressed in the first draft of the General Data Protection Regulation revealed in 2012—two years before the Court of Justice's decision in Google Spain. *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of*

Rather, the Court of Justice's declaration of the right required some "creative manipulation" of the DPD.[163] Although the right itself sprouts from the privacy and data protection rights recognized in the Convention, Charter, and Directive,[164] the rights granted to data subjects in the DPD do not track the "inadequate, irrelevant or no longer relevant, or excessive" language used in the *Google Spain* decision.[165]

Moreover, the DPD nowhere compels data controllers to balance fundamental rights in an adjudicatory fashion. Rather, it provides a "right to obtain *from the controller* . . . as appropriate the rectification, erasure or blocking" of data processing,[166] but makes the balancing of such requests against expressive freedom a national obligation. "*Member States* shall provide for exemptions or derogations" with respect to freedom of expression.[167] Thus, the Directive charges data controllers with the obligation to erase, but it charges member states with the obligation to provide free expression exceptions. If anything, the Directive envisions data controllers complying with national decisions to block, erase, or destroy rather than those data controllers making those decisions themselves. The Directive entrusts data protection authorities with "ordering the blocking, erasure or destruction of data"[168] and "hear[ing] claims . . . concerning the protection of . . . rights and freedoms in regard to the processing of personal data,"[169] again suggesting that the proper adjudicator is not the data processor but the member states' data protection authorities.

B. THE PRECARIOUS IMPLEMENTATION OF THE *GOOGLE SPAIN* RIGHT TO BE FORGOTTEN HIGHLIGHTED INCONSISTENT TRANSATLANTIC DATA PRIVACY VALUES

In the wake of the landmark legal decision, Google and other data

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 17, COM (2012) 11 final (Jan. 25, 2012) [hereinafter January 2012 GDPR Text].

163. Krotoszynski, *supra* note 60, at 1329. *But see* Recent Case, *supra* note 74, at 741 (noting "the clear tie between the court's decision and the Directive's text and values.").

164. Siry, *supra* note 31, at 328. *See supra* Part I.A.

165. Directive, *supra* note 34, arts. 12(b), 14(a). The language appears to derive from Article 6 in a section regarding data quality, not the rights of data subjects. Article 6(1) provides that "Member states shall provide that personal data must be: . . . (c) adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed." *Id.* art. 6(1).

166. *Id.* art. 12 (emphasis added).

167. *Id.* art. 9 (emphasis added).

168. *Id.* art. 28(3).

169. *Id.* art. 28(4).

controllers scrambled to implement right-to-be-forgotten adjudicatory instruments. The Article 29 Data Protection Working Party ("Working Party"), a group created by the DPD to advise on data privacy issues,[170] suggested some contours to the balancing test and explicitly referred to the freedom of expression and information right guaranteed in Article 11 of the Charter.[171] The Working Party confirmed that right-to-be-forgotten delisting decisions are within search engine operators' decisionmaking capacity, and that formal claims under the Directive—claims subject to national data protection authorities' review—are not established until search engines provide "refusals or partial refusals" of right-to-be-forgotten requests.[172]

Meanwhile, in response to the *Google Spain* decision, Google convened an Advisory Council to adapt to the unfamiliar European rights-balancing test.[173] The Advisory Council identified evaluative criteria for erasure requests[174] and embraced the adjudicatory function thrust upon search engines.[175] It declared that the adjudicatory role Google and other intermediaries play with respect to erasure requests "is already the norm" in other legal contexts.[176] But Google declined to extend the domain of delistings outside the national search portal of the delisting requestor (that is, delisting results from google.fr but not from google.com or google.de),[177] citing "the legal principle of proportionality and extraterritoriality in application of European law."[178] Its delisting request form thus requires data subjects to select the "[c]ountry whose law applies to your request,"[179] reflecting its commitment to limited territorial

170. *Id.* art. 29.

171. *See* Working Party Implementation Guidelines, *supra* note 50, ¶ 8.

172. *Id.* ¶¶ 20, 24.

173. *See Google Advisory Council*, GOOGLE, https://archive.google.com/advisorycouncil (last visited Aug. 14, 2017) ("We want to strike this balance right. This obligation has been a new and difficult challenge for us, and we've sought advice on the principles Google ought to apply when making decisions on individual cases.").

174. *See* ADVISORY COUNCIL, *supra* note 15, at 7–14 (including in its list of criteria the data subject's "role . . . in public life," the "nature of the information" requested to be delisted, "the source of that information and the motivation for publishing it," and the amount of time elapsed since the publication of the information).

175. *See id.* at 25 (Leutheusser-Schnarrenberger comments) ("This right to decide cannot be taken away from the company.").

176. *Id.* at 18 (analogizing to copyright and child-abuse image delinking).

177. *Id.* at 18–20.

178. *Id.* at 20. *Contra id.* at 27 (Leutheusser-Schnarrenberger comments) ("The internet is global, the protection of the user's rights must also be global. Any circumvention of these rights must be prevented. Since EU residents are able to research globally the EU is authorized to decide that the search engine has to delete all the links globally.").

179. *EU Privacy Removal*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=

application as well as the assortment of national data protection laws proliferating under the DPD.

European data protection advisors and authorities promptly rejected such approaches. In its enforcement guidelines advising national data protection authorities on enforcement of *Google Spain*, the Working Party recommended that delistings should extend globally:

> [D]e-listing decisions must be implemented in a way that guarantees the effective and complete protection of these rights and that EU law cannot be easily circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.[180]

In June 2015, the French data protection authority declared that it would enforce global delisting across all domains, reasoning that effective erasure was impossible otherwise.[181] Google refused to comply with the French authority's order to extend delistings to all Google domains, and the authority rejected an informal appeal of the order.[182] Google continues to reject European authorities' extraterritorial application of the DPD.[183]

As the European Union approaches comprehensive data protection reform and harmonization, including an express right to erasure,[184] Google and other intermediaries are already facing a clash of disparate data privacy regimes on either side of the Atlantic in the form of the *Google Spain* decision.[185] The Court of Justice delegated adjudicatory authority over the balancing of European fundamental rights to data controllers, many of whom are from the United States, where such rights-balancing is unrecognized. American data controllers are expected to value privacy over

websearch (last visited Aug. 14, 2017).

180. Working Party Implementation Guidelines, *supra* note 50, ¶ 20.

181. *CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine*, CNIL (Jun. 12, 2015), http://www.cnil.fr/fr/node/15790.

182. *Right to Delisting: Google Informal Appeal Rejected*, CNIL (Sep. 21, 2015), http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected. Google proposed to settle the dispute over the global delisting issue by honoring delisting requests across all Google domains, but restricting delistings by geolocation to only searches from Internet protocol addresses from the European Union. Rick Mitchell, *Google Right to Forget Amendment Plan Faces Skepticism*, BLOOMBERG BNA (Mar. 2, 2016), http://www.bna.com/google-right-forget-n57982068042.

183. *EU Privacy Removal*, *supra* note 179.

184. GDPR, *supra* note 23, art. 17.

185. *See* Rustad & Kulevska, *supra* note 30, at 376.

their economic interests, and often over the interest of the general public in having unimpeded access to information—the trade in which data controllers like Google specialize. And with the specter of global delisting enforcement from both the *Google Spain* decision and the proposed GDPR right to erasure, the European Union is exporting data protection rules and rights valuations without considering the reconcilability of transatlantic privacy regimes.

III. THE NEW, FLAWED RIGHT TO ERASURE WILL FAIL TO EXPAND THE *GOOGLE SPAIN* EXERTION OF EUROPEAN PRIVACY VALUES

After years of trilogue negotiations between the European Parliament, European Commission, and Council of Ministers,[186] the Parliament and the Council adopted the GDPR in April 2016.[187] The Regulation, which will take effect in May 2018,[188] aims to harmonize data protection laws across European member states.[189] It also effectively overrides *Google Spain*, as that decision was premised on the DPD that the Regulation replaces.[190]

But the privacy policy exertions of the European Court of Justice decision still will influence the tenor of the relationship between the data privacy regimes and serve as harbingers of the new European system. The 2014 *Google Spain* decision was at least in part influenced by the draft of the GDPR circulated in January 2012, and it may have served as a pilot program for the right eventually included in the final text.[191] Moreover, the GDPR generally adopts all references to the Directive as references to the Regulation.[192]

Despite the harmonizing aim of the Regulation and the influence of the *Google Spain* decision on privacy valuation for U.S.-based companies, the GDPR falls short by permitting derogations for free expression dependent on the national laws of European member states. Instead of providing a unified exportation of the right to be forgotten across the Atlantic, the Regulation leaves free expression exceptions to the privacy

186. *See* Burton et al., *supra* note 22.

187. GDPR, *supra* note 23.

188. *Id.* art. 99(2).

189. European Commission Statement 15/5257, *supra* note 22.

190. *See* GDPR, *supra* note 23, art. 94.

191. *See* Marcus Evans et al., *The European Court of Justice Rules on the "Right to Be Forgotten,"* LEXOLOGY (May 19, 2014), http://www.lexology.com/library/detail.aspx?g=3f9ddd42-5414-41ec-b719-235ab7b16fa1.

192. GDPR, *supra* note 23, art. 94(2).

interest fragmented at the national level.[193] Thus, American companies subject to the jurisdictional pull of the Regulation can still avoid the European Union's coequal valuation of privacy and expression by strategically locating their European headquarters in countries that have data protection supervisory authorities that favorably weigh these national freedom of expression laws.[194] This architectural flaw in the Regulation promises to limit the effectiveness of any gambit to pull U.S. privacy values toward European norms through the Regulation's right to erasure.

A. THE EVOLUTION OF THE RIGHT TO ERASURE IN THE GDPR

As a regulation rather than a directive, the GDPR will have the force of law in all EU member states, not requiring national legislation to implement.[195] (In contrast, the DPD merely set out principles that member states were required to implement on a national level.[196]) Thus, member state data protection authorities have different national standards, causing dissonance within the European Union despite the unified goals of the Directive. For example, the French data protection authority has been especially stringent in enforcing *Google Spain* delisting requests globally—not just in the European Union.[197] Although many member states have similar standards, national variations complicate the Directive's data protection system.

The GDPR harmonizes those twenty-eight member state laws and seeks to overhaul the European data privacy system. The Regulation is estimated to save €2.3 billion over the DPD scheme through this harmonization.[198] The Regulation better defines the right to erasure just as it expands the jurisdictional reach of the European data protection rules.[199]

The Regulation treats enforcement of the right to erasure very seriously. Infringements of the Regulation can cost a controller up to 4 percent of its "total worldwide annual turnover of the preceding financial

193. *See infra* Part III.B.

194. *See infra* Part III.C & Conclusion.

195. *Regulations, Directives and Other Acts*, *supra* note 85.

196. *See* Directive, *supra* note 34, art. 4.

197. *Right to Delisting: Google Informal Appeal Rejected*, CNIL (Sep. 21, 2015), https://www.cnil.fr/fr/node/15814.

198. European Commission Memo 15/6385, Questions and Answers—Data Protection Reform (Dec. 21, 2015), http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.

199. *See* GDPR, *supra* note 23, art. 3; Keller, *supra* note 16 ("The GDPR asserts jurisdiction over entities that offer services to or 'monitor' EU users. 'Monitoring' seems to be defined broadly enough to include fairly standard web and app customization features, so the law reaches many online companies outside of the EU.").

year."[200] This penalty can be imposed for violations of a data subject's privacy rights, including the right to be forgotten.[201] When such a high penalty can be levied against a controller for a single infringement of a single data subject's privacy rights—in the case of Google, up to $3.6 billion per infringement[202]—the cost of incorrectly adjudicating against erasure can be devastating.

B. THE RIGHT TO ERASURE CONTAINS NATIONAL EXPRESSION DEROGATIONS THAT ERODE THE HARMONIZATION AIMS OF THE REGULATION

Article 17(1) of the Regulation outlines the basic rule: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" in specific outlined circumstances.[203] For example, a data controller must honor an erasure request if the data are no longer necessary, if the data subject withdraws consent for data processing, or if the data "have been unlawfully processed."[204]

It is noteworthy that the right has developed significantly since the initial January 2012 draft of the regulation and the *Google Spain* decision. The January 2012 draft specified that the right may be appropriately exercised for "personal data which are made available by the data subject while he or she was a child," though it did not restrict the exercise of the erasure right exclusively to children.[205] Moreover, the right to erasure as contemplated in the final text of the Regulation does not specifically refer to the "inadequate, irrelevant or no longer relevant, or excessive" standard put forth in the DPD in *Google Spain*.[206] Thus, the final text of the Regulation suggests a broader right than the one being adjudicated under the DPD regime.

200. GDPR, *supra* note 23, art. 83(5).

201. *Id.* art. 83(5)(b).

202. *See Alphabet Inc*, GOOGLE FIN., https://www.google.com/finance?q=NASDAQ:GOOG&fstype=ii (last visited Aug. 14, 2017) (showing a revenue of $90.272 billion in fiscal year 2016).

203. GDPR, *supra* note 23, art. 17(1).

204. *Id.* art. 17(1)(a), (b), (d).

205. January 2012 GDPR Text, *supra* note 162, art. 17(1).

206. *See supra* note 165 and accompanying text. The GDPR does include language requiring processed personal data to be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')," though "data minimisation" does not refer specifically to the right to be forgotten but to data processing generally. GDPR, *supra* note 23, art. 5(1)(c). *Cf.* Directive, *supra* note 34, art. 6(1).

Nevertheless, the right is checked by principles of free expression, recalling the privacy-expression balancing underpinning European fundamental rights adjudication. The right to be forgotten "shall not apply to the extent that processing of the personal data is necessary . . . for exercising the right of freedom of expression and information."[207] But that expression right is not defined in the context of Article 17. Instead, the "freedom of expression and information" is contemplated in Article 85 of the Regulation, which relegates expression derogations to member states.[208] The member states are tasked with "reconcil[ing] the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including the processing [of personal data] for journalistic purposes and the purposes of academic, artistic or literary expression."[209]

Recital 153 sheds some light on what happens if member state expression laws conflict. The Regulation suggests that:

> Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. . . . Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply.[210]

Thus, even though the GDPR harmonizes member state law in providing a uniform right to erasure, the right remains fragmented in the implementation of the free expression derogation. This fragmentation is further complicated because determining the member state law which data controllers must apply when adjudicating the erasure right is not straightforward.

C. ONE-STOP-SHOP FORUM-SELECTION PRINCIPLES MANIFEST IN ODD OVERSIGHT CONFIGURATIONS

The GDPR includes provisions that allow data controllers to control which "supervisory authority" (that is, which national data protection

207. GDPR, *supra* note 23, art. 17(3)(a).

208. *Id.* art. 85(2) ("For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from . . . Chapter III (rights of the data subject)," which include the Article 17 right, "if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information."). The initial draft of the Regulation made specific reference to this Article, then numbered Article 80, in Article 17. January 2012 GDPR Text, *supra* note 162, art. 17(3)(a).

209. GDPR, *supra* note 23, art. 85(1).

210. *Id.*, recital 153.

authority) will take point on most appeals of erasure decisions.[211] Despite some limits to these "one-stop-shop" measures, this gambit to reduce the administrative burden borne by controllers will effectively give them power to select the data protection authorities whose adjudication is most consistent with the United States' valuation of free expression.

The European Council illuminates the purposes behind the new one-stop-shop rules:

> [T]he regulation should establish a "one-stop-shop" mechanism in order to arrive at a *single supervisory decision*, which should be *fast*, ensure *consistent application*, provide *legal certainty* and *reduce the administrative burden*. . . . [T]he *one stop shop mechanism should only play a role in important cross-border cases* and will provide for cooperation and joint-decision making between several data protection authorities concerned.[212]

The Regulation carries out these goals by giving preference to the national authority of the member state in which the main establishment of the controller is located. Where a controller engages in cross-border processing of personal data, "the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority."[213] Other national authorities are relegated to the role of a "supervisory authorit[y] concerned."[214] Article 56 affords much more autonomy and authority to the lead authority than to the concerned authorities. Although the lead authority must cooperate diligently with the concerned authorities,[215] the lead authority drafts decisions and communicates with the controller.[216] Thus, when an erasure decision made by a controller is appealed, the lead supervisory authority is the one that takes point.

But the lead supervisory authority does not have ultimate authority over rights adjudication under the GDPR, unlike under the DPD.[217] The

211. GDPR, *supra* note 23, chs. VI–VII.

212. European Council Press Release 15/114, Data Protection: Council Agrees on General Principles and the "One Stop Shop" Mechanism (Mar. 13, 2015), http://www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism.

213. GDPR, *supra* note 23, art. 56(1). Where a controller has establishments in multiple member states, the main establishment is "the place of [the controller's] central administration in the Union" or where decisions on the purposes and means of personal data processing take place. *Id.* art. 4(16).

214. *See id.* art. 60.

215. *E.g.*, *id.* arts. 60–62.

216. *Id.* art. 56.

217. *See* Directive, *supra* note 34, art. 28.

supervisory authorities must work in concert, and concerned authorities may lodge objections with the lead authority.[218] Moreover, the supervisory authorities are all organized under the European Data Protection Board, which has ultimate authority over the Regulation's implementation, serves as the court of last resort, and resolves disputes among supervisory authorities.[219]

Nevertheless, the designation of lead supervisory authorities provides a default contact point for controllers to navigate the European data privacy system under the Regulation. It also interacts with the continued fragmentation of national free expression laws. A lead supervisory authority must apply the member state law to which the controller is subject, which can be the law of the lead supervisory authority's home state or that of any other member state, depending on the national origin of the data subject requesting erasure.[220] Because expression laws are national and may apply no matter where the main establishment of the controller is located, national lead supervisory authorities will be tasked with applying foreign member state law in adjudicating privacy rights.[221] Consider this situation: erasure adjudication can require the French supervisory authority, weighing an erasure request directed at a U.S.-based company with headquarters located in Ireland, to balance Estonian expression values against pan-European privacy values. It is entirely possible—if not inevitable—for this to happen under the one-stop-shop principles.

The GDPR goes above and beyond the DPD in harmonizing rules across European data markets, but the awkward adjudicatory issues the GDPR creates stymie its ultimate effect.[222] The Regulation makes big strides, but it does not go far enough; data protection touches many different, interlocking values. Just examining the values of privacy and expression weighed in erasure adjudication, the lack of total harmonization of free expression derogations to a unified erasure rule impedes the efficacy of the Regulation.

218. GDPR, *supra* note 23, art. 60(1)–(4).

219. *Id.* arts. 65(1)(a)–(b), 70(1).

220. *See id.* recitals 65, 153.

221. Marcus Evans & Adam Smith, *Dispute Resolution Mechanisms for SAs and Individuals Are Key Part of Proposed EU Regulation*, DATA PROTECTION REP. (Apr. 21, 2015), http://www.dataprotectionreport.com/2015/04/dispute-resolution-mechanisms-for-sas-and-individuals-are-key-part-of-proposed-eu-regulation.

222. *See* Kevin Gallagher, *EU Council's Agreement and the "One-Stop Shop,"* ILI STUDENT BLOG (Apr. 16, 2015, 4:58 PM), http://blogs.law.nyu.edu/privacyresearchgroup/2015/04/eu-councils-agreement-and-the-one-stop-shop.

CONCLUSION

Data controllers tasked with implementing the right to be forgotten face twenty-eight different freedom of expression laws and twenty-eight different supervisory authorities in twenty-eight different states, each of which may pull the controller into the orbit of its national law.[223] American companies with flourishing business in European data markets face a conundrum. When Europe approaches data protection from a perspective with which Americans are unfamiliar—balancing privacy and expression coequally[224]—how is a U.S.-based company supposed to adapt? What can it do when it has to adjudicate hundreds of thousands of erasure requests from around the European Union[225] and when it risks billions of dollars in penalties every single time it makes a decision not to forget?[226]

Data-driven US companies can utilize the adjudicative and jurisdictional messes the GDPR creates to their advantage.[227] Although all American controllers of European personal data are subject to the jurisdiction of the pan-European Regulation and its harmonized data privacy values, they are not subject to pan-European free expression laws.[228] Moreover, U.S. controllers take the first shot at adjudicating the erasure right,[229] and only upon appeal does a national supervisory authority get involved.[230]

The European Union made grand gestures in recent years, indicating that its new Regulation would serve as another strategic move pushing the American data protection regime, inch by inch, toward adopting European privacy values.[231] With the adoption of a right to be forgotten in *Google Spain* as a pseudo–pilot program, Europe was poised to use the GDPR as an instrument of converging European and American data protection systems.[232]

But the Regulation falls short of doing that. It effectively allows U.S. data controllers to bypass the stringent requirements of the right to erasure

223. *See supra* Part III.B.

224. *See supra* Part I.A.

225. For a continuing count of "URLs Requested and Delisted," see *Search Removals Under European Privacy Law*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/eu-privacy/overview (last visited Aug. 15, 2017).

226. *See supra* notes 200–02.

227. *See supra* Part III.

228. *See supra* Part III.B.

229. *See supra* Parts II.A & III.A.

230. *See supra* Part III.C.

231. *See supra* Part II.

232. *See id.*

under the Regulation by selectively shopping for the lead supervisory authority that treats the expression derogation in the right to be forgotten most favorably. Essentially, U.S.-based companies can focus economic and political pressure on a single member state and its supervisory authority to be the arbiters of privacy-expression disputes under the Regulation. American companies can rally around the selected member state, locate their European headquarters in that state, and focus lobbying efforts regarding appeals of the erasure right on that member state.

Enter Ireland.[233] "All of the top 10 U.S. companies that were born on the Internet—including Google, Amazon and eBay—have overseas corporate headquarters in Ireland."[234] Ireland enjoys a wealth of technology investments from U.S.-based companies.[235] The plain reason for this is that Ireland offers a low corporate tax rate,[236] but the overwhelming influence of American companies in the EU member state has created a virtuous cycle reinforcing the community of U.S. controllers centering their European operations in the member state.[237] And the Irish Data Protection Commissioner is "very aware" of this fact.[238]

The Regulation will not take effect until 2018, but it is foreseeable that its effectiveness in pushing American privacy values closer to European ones may be limited. Given the flaws in the architecture of the GDPR, it is not far-fetched to conclude that Ireland—or any other amenable member state—could serve as U.S. companies' "single nominated authority that could rule on large or politically contentious data protection issues."[239] "[F]orcing convergence of national law in this way is a lengthy process, particularly for new and fast-moving areas of technology like cyberspace."[240] The GDPR will not be the convergent force that brings the

233. *See* Samuel Gibbs, *EU States Agree Framework for Pan-European Data Privacy Rules*, GUARDIAN (June 15, 2015, 9:46 AM), http://www.theguardian.com/technology/2015/jun/15/eu-privacy-laws-data-regulations.

234. Ari Shapiro, *U.S. Tech Firms See Green as They Set Up Shop in Low-Tax Ireland*, NAT'L PUB. RADIO (Dec. 8, 2014, 4:16 AM), http://www.npr.org/sections/parallels/2014/12/08/368770530/u-s-tech-firms-see-green-as-they-set-up-shop-in-low-tax-ireland.

235. *Id.*

236. Martin Bryant, *What Attracts Big Tech Companies to Ireland? Hint: It's Not Just Low Taxes*, NEXT WEB (Nov. 26, 2011), http://thenextweb.com/insider/2011/11/26/what-attracts-big-tech-companies-to-ireland-hint-its-not-just-low-taxes.

237. Martin Sullivan, *If Ireland Is Not a Tax Haven, What Is It?*, FORBES (Nov. 6, 2013, 09:57 AM), http://www.forbes.com/sites/taxanalysts/2013/11/06/if-ireland-is-not-a-tax-haven-what-is-it/#2d917a913355.

238. Ali Qassim, *Irish Companies Set Data Transfer, EU Reg Priorities*, BLOOMBERG BNA (Feb. 29, 2016), http://www.bna.com/irish-companies-set-n57982067880.

239. Gibbs, *supra* note 233.

240. CHRIS REED, MAKING LAWS FOR CYBERSPACE 38 (2012).

United States into the European privacy mold.