Harvard Journal of Law & Technology
Volume 28, Number 2 Spring 2015

RECONCEPTUALIZING THE RIGHT TO BE FORGOTTEN TO ENABLE TRANSATLANTIC DATA FLOW

*Michael L. Rustad & Sanna Kulevska**

TABLE OF CONTENTS

---

* This Article draws ideas from Sanna Kulevska's graduate thesis, *Humanizing the Digital Age: A Right To Be Forgotten Online? — An EU-U.S. Comparative Study of Tomorrow's Privacy in Light of the General Data Protection Regulation and* Google Spain v. AEPD, at the Faculty of Law at Lund University in Sweden in 2014 and her academic paper on the EU right to be forgotten supervised by Professor Michael Rustad at Suffolk University Law School in his Emerging Issues in Information Technology seminar in the fall of 2012. The authors also extend ideas introduced in Professor Rustad's book, GLOBAL INTERNET LAW (HORNBOOK SERIES) (2d ed. 2014).

Professor Rustad is the Thomas F. Lambert Jr. Professor of Law, which was the first endowed chair at Suffolk University Law School. He is Founding Director and current Co-Director of Suffolk's Intellectual Property Law Concentration and was the 2011 Chair of the American Association of Law Schools Torts and Compensation Systems Section. Professor Rustad has more than 1200 citations on Westlaw. His most recent books are SOFTWARE LICENSING: PRINCIPLES AND PRACTICAL STRATEGIES (2d ed. 2014), GLOBAL INTERNET LAW (HORNBOOK SERIES) (2d ed. 2014), and GLOBAL INTERNET LAW IN A NUTSHELL (2d ed. 2013). He is the editor of the five volume edition of COMPUTER CONTRACTS: NEGOTIATING AND DRAFTING (2015).

Sanna Kulevska is a Swedish lawyer who graduated in June 2014 after law studies at the Faculty of Law at Lund University in Lund, Sweden as well as Suffolk University Law School in Boston, United States. She is currently working at the Legal Department of Google's European Headquarters in Dublin, Ireland. Prior to this position, Sanna Kulevska worked at the Headquarters for Global Intellectual Property Law at the adidas Group in Amsterdam, the Netherlands. In 2013, she was a Legal Research Assistant at the Chilling Effects Clearinghouse at Harvard University's Berkman Center for Internet and Society, where she worked on projects related to takedown requests of personal online data and cyber defamation. She also interned at Duane Morris LLP, a leading international intellectual property and entertainment law firm as well as at the U.S. litigation law firm Sweder & Ross LLP. This Article was accepted by the *Harvard Journal of Law & Technology* in August 2014, prior to Sanna Kulevska's employment at Google beginning December 1, 2014. It must therefore be emphasized that this Article is solely based on the original and independent academic writing and analysis of the authors, and it is neither a Google product nor a reflection of Google's legal policy.

The authors would like to thank Professor Rustad's research assistant Naphtalia Lafontant for her helpful research and editorial proposals. Professor Rustad would also like to thank his wife Chryss J. Knowles for reviewing the manuscript and Sanna Kulevska would like to thank her family for their invaluable love and support. Finally, the authors would like to thank Sheri Pan, *Harvard Journal of Law & Technology* Article Editor, for her insightful editorial suggestions.

I. INTRODUCTION

Today, children around the world create perpetual digital footprints on social network websites on a 24/7 basis as they learn their ABCs: Apple, Bluetooth, and Chat followed by Download, E-Mail, Facebook, Google, Hotmail, and Instagram. Eric Schmidt, Executive Chairman of Google, has stated that we are creating the equivalent amount of information every other day as all of humanity created from the beginning of recorded history to 2003, and this is in large part enabled by the World Wide Web.[1] "[G]lobal IP traffic will reach 1.1 zettabytes per year" by 2016, "or 91.3 exabytes (one billion gigabytes) per month, and by 2018, global IP traffic will reach 1.6 zettabytes per year or 131.9 exabytes per month."[2]

---

1. *See* M.G. Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003*, TECHCRUNCH (Aug. 4, 2010), http://techcrunch.com/2010/08/04/schmidt-data/.

2. *The Zettabyte Era — Trends and Analysis*, CISCO (June 10, 2014), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html; *see also* John Gantz & David Reinsel, *The Digital Universe in*

The human brain's ability to forget is as critically important to consciousness as the ability to recall. *Stedman's Medical Dictionary* defines human forgetting as "being unable to retrieve or recall information that was once registered, learned, and stored in short-term or long-term memory."[3] Forgetting is useful because it enables humans to adjust and reconstruct memories, to generalize, and to construct abstract thoughts.[4] If humans could always remember data, dreams, or daily experiences, the ocean of information would soon inundate the brain's network of synapses.[5] The human brain consists of a hundred billion neurons that process information[6] and lacks the capability to store every single stimulus received,[7] in contrast to the practically infinite storage space of the Internet. Selective memory is adaptive, giving human data subjects a way to shed their past and start fresh: We can forgive and forget.

Unlike the human brain with its imperfections and forgetfulness, the web recollects nearly everything and everyone.[8] Information is perpetually accessible, and data subjects have limited ability to conceal past transgressions.[9] Now we are switching to a system in which the Internet is a treasure trove of immutable memories and data subjects must take extraordinary steps in order to forget. That is an enormous transformation. Social media postings that go viral permanently stigmatize by creating a "digital Scarlet letter," which is "an indelible record of people's past misdeeds . . . . The Internet is indeed a cruel historian."[10]

Current as well as future employers routinely search the Internet to cybervet prospective employees.[11] Social networks, for example,

---

2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, INTERNET DATA CORP. (Dec. 2012), http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf ("From 2005 to 2020, the digital universe will grow by a factor of 300, from 130 exabytes to 40,000 exabytes, or 40 trillion gigabytes (more than 5,200 gigabytes for every man, woman, and child in 2020).").

3. STEDMAN'S MEDICAL DICTIONARY 348060 (27th ed. 2000), *available at* Stedman's Medical Dictionary 348060 (Westlaw).

4. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 118 (2009); *see also* Focus on Memory, 16 NATURE NEUROSCIENCE 111, 111 (2013) ("From the moment they are created, [memories] . . . are consolidated, often updated, but also sometimes distorted to the point that they falsify the past. As our brain is constantly bombarded with newer information, memories may also become suppressed by competing memories or experiences or seemingly disappear into oblivion.").

5. MAYER-SCHÖNBERGER, *supra* note 4, at 17; *see also* Joshua Foer, *Remember This*, NAT'L GEOGRAPHIC MAG. (Nov. 2007), http://ngm.nationalgeographic.com/2007/11/memory/foer-text (explaining the value of biological forgetting).

6. MAYER-SCHÖNBERGER, *supra* note 4, at 16.

7. Foer, *supra* note 5.

8. MAYER-SCHÖNBERGER, *supra* note 4, at 10–11.

9. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 11 (2007).

10. *Id.*

11. Expert Report at 1, *In re* McClenaghan v. Turi, 2012 WL 6212498 (E.D. Pa. 2012) (No. 09-cv-05497-PBT) ("[I]t is well documented that a high percentage of employers now

augment human memory by collecting, processing, and storing our status updates or tweets that may stigmatize or embarrass when viewed out of context. Sociologist Erving Goffman explained how stigmatized persons managed offline identities that had been compromised by physical handicap, mental disorder, unemployment, or conviction.[12] Internet postings, comments, and pictures create a permanent stigmatization, as it is now impossible to forget.[13] Remembering, not forgetting, is the new default in the Internet epoch.[14]

On January 1, 2012, the European Commission published the Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("GDPR"), which updates the former Data Protection Directive to fortify privacy rights for the citizens of the European Union.[15] This unified regulation will give all European Union citizens a right to be forgotten online,[16] a right for the individual user to have his or her personal online data removed from the web.[17] The Court of Justice of the European Union ("CJEU") jumpstarted Europe's recognition of the right to be forgotten by reading a right to be forgotten into the extant Data Protection Directive in a May 2014 decision, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*[18] (*Google Spain v. AEPD*). The court's decision in *Google Spain v. AEPD* recognized the right of a Spanish citizen to have personal data about his insolvency delinked so

---

utilize online search to research and investigate potential employees . . . . Unlike formal background checks that require an applicant's written authorization prior to search, the Internet delivers unfiltered search results . . . .").

12. *See generally* ERVING GOFFMAN, STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY (1963).

13. Chris Conley, *The Right To Delete*, AAAI SPRING SYMPOSIUM: INTELLIGENT INFORMATION PRIVACY MANAGEMENT 53, 53 (2010), *available at* https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482.

14. *Id.*

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

16. "The right to be forgotten" is a data privacy concept which has been discussed in Argentina since 2006, *see* Vinod Sreeharsha, *Google and Yahoo Win Appeal in Argentine Case*, N.Y. TIMES (Aug. 19, 2010), http://www.nytimes.com/2010/08/20/technology/internet/20google.html?_r=0, and can be described as a desire for individuals to "determine the development of their lives in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past," Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the "Right To Be Forgotten,"* 29 COMPUTER L. & SEC. REV. 229, 229–35 (2013).

17. *GDPR*, *supra* note 15, art. 17. *See generally* Press Release, Eur. Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

18. Case C-131/12, Google Spain SL. v. Agencia Española de Protección de Datos (May 13, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

that this information would not appear in response to a search for his name in a search engine.[19] In this high profile case, the Court classified Google as a controller of personal data and thereby responsible for removal of the information.[20]

This Article examines the implications of the *Google Spain* case as well as the full-blown impact of the proposed GDPR that is estimated to go into effect in the European Union in 2017.[21] The central problem with the right to be forgotten as conceptualized by the CJEU and the Commission is that the expansiveness of the right threatens to cannibalize free expression.[22] Thus, this Article calls for a shrinking of the right to be forgotten to appropriately balance the right of data subjects to control personal information about themselves with free expression and the public interest in preserving history. We propose that the EU Commission operationalize free expression by narrowing the right to be forgotten for private persons, public officials, and public figures. Private persons will have the right to delete links to their own postings and repostings by third parties. They will have a right to delete links to postings created by third parties upon proof that the information serves no legitimate purpose other than to embarrass or extort payment from the data subject. Public officials and public figures will have a right to remove links to their own postings and repostings by third parties, but not postings about them by third parties, unless the third party was acting with actual malice and the posting does not implicate the public's right to know.[23] In addition, all right to be forgotten requests will be subject to a general exemption for the public's right to know.

---

19. *Id.* ¶¶ 14, 72, Ruling ¶¶ 1–4.

20. *Id.* ¶¶ 32–34 ("It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing . . . .").

21. Susan L. Foster, *Timing Update for the EU Data Protection Regulation: No News Doesn't Mean It's Gone Away*, NAT'L L. REV. (July 24, 2014), http://www.natlawreview.com/article/timing-update-eu-data-protection-regulation-no-news-doesn-t-mean-it-s-gone-away.

22. We would like to emphasize that freedom of expression in this Article includes freedom of speech as well as freedom to seek and impart information as stated in, for example, the Universal Declaration of Human Rights Article 19 and the European Convention of Human Rights Article 10. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 10, U.N. Doc. A/RES/217(III), at 74–75 (Dec. 10, 1948) [hereinafter UDHR], *available at* http://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx; Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR], *available at* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

23. *See* New York Times Co. v. Sullivan, 376 U.S. 254 (1964); Curtis Publ'g Co. v. Butts, 388 U.S. 130 (1967); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974). Although the Article only addresses the private person, public official, and public figure criterion, there are other criteria that search engines consider, such as whether the posting is stale, involves a minor, or relates to a crime. Rather than presenting a complete template for deciding whether or not to accept a delisting request, the Article focuses on the reconciliation of freedom of expression and information with the right to be forgotten.

Part I of this Article introduces how the Internet's vast storage capacity renders a data subject's online postings, comments, and pictures a permanent digital record. Forgetting, rather than remembering, is the problem for data subjects who must wear a digital scarlet letter for stigmatizing information posted on the Internet.

Part II traces the development of the concept of the right to be forgotten under European law by examining the 1995 Data Protection Directive ("Directive 95/46/EC"), the CJEU decision in Google Spain v. AEPD, and the proposed GDPR.

Part III examines the reasons why the right to be forgotten failed to develop under United States law. Americans are from Mars and Europeans are from Venus when it comes to data privacy and the right to be forgotten.[24] In this part of the Article, we compare the EU and U.S. privacy regimes and explain how the EU's right to be forgotten, as currently framed, is antithetical to the First Amendment of the U.S. Constitution. Because personally identifiable data crosses from Europe to the United States at the click of the mouse, there is a great need to harmonize the right to be forgotten between these two important trading partners in an information-based economy.

In Part IV, we propose non-legislative solutions to supplement the scaled down right to be forgotten. In addition to a right to be forgotten where search engines such as Google or Bing delink stories about the data subject, we propose best practice agreements, expiration dates for personally identifiable data, the widespread use of contextualization, and cognitive adjustment. These measures will supplement but not supplant the formal legal right to be forgotten that we discuss in Part V.

Part V proposes an EU-U.S. harmonization of the right to be forgotten to enable transatlantic data flow while protecting the freedom of expression. The EU Commission already recognizes that the right to be forgotten is not absolute and is subject to the freedom of expres-

---

24. *See* Michael L. Rustad & Maria V. Onufrio, *Reconceptualizing Consumer Terms of Service for a Globalized Knowledge Economy*, 14 U. PA. J. BUS. L. 1085, 1189 (2012).

> Robert Kagan's article in The Economist entitled 'Old America v. New Europe,' explodes the naive assumption that Europe is a [sic] an old continent while America is a mere teenager. America's political system is a senior citizen compared to the upstart European Union. The golden age of U.S.-style TOUs [Terms of Use] may be coming to an end because of the increasingly flattened world in which U.S. companies license content to European consumers. The United States is like Mars and Europe like Venus when it comes to consumer rights for TOUs. When it comes to the reform of unjust rules such as those enforced in the United States, it will not do to simply 'let the market solve the problem.'

Id.; *see also* Ivo H. Daalder, *Books of the Times; Americans Are from Mars, Europeans from Venus*, N.Y. TIMES (Mar. 5, 2003), http://www.nytimes.com/2003/03/05/books/books-of-the-times-americans-are-from-mars-europeans-from-venus.html.

sion in Article 17(3) of the GDPR.[25] We propose formalizing the recognition of the freedom of expression by adopting U.S.-style rules for limiting the right to be forgotten for private persons, public officials, and public figures, where there is a strong public right to know. Any broader right to be forgotten abridges free expression, censors the Internet, and rewrites history.

II. HIDING FROM HISTORY: THE EUROPEAN RIGHT TO BE FORGOTTEN

A. Early Developments in European Privacy

1. The Treaty of Lisbon and Privacy

The right of privacy is a comprehensive, fundamental, and constitutional right throughout the European community. The European Union launched the "'Lisbon Agenda' with the goal of making Europe the most competitive and dynamic knowledge-driven economy in the world."[26] The Treaty of Lisbon is the international agreement that updated the constitutional framework for the European Union and affirmed the worth of "human dignity, freedom, democracy, equality, the rule of law and respect for human rights."[27] The rights to privacy and self-determination in EU countries extend to both private and public sector data processors[28] and apply to all industries, as opposed to the sectorial protection found in the United States.[29] Additionally, privacy in the European Union originated as a right of individual consent, something that later evolved into the individual's right to participate in society.[30]

---

25. *GDPR*, *supra* note 15, art. 17(3), at 52.

26. Jane K. Winn, *Technical Standards as Data Protection Regulation*, *in* REINVENTING DATA PROTECTION 201 (Serge Gutwirth et al. eds., 2009).

27. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community art. 1a, Dec. 13, 2007, 2007 O.J. (C 306) 1, 12.

28. Robert Roskin, *UK: Data Controllers and Data Processors: What Is the Difference?*, MONDAQ (June 16, 2014), http://www.mondaq.com/article.asp?articleid=320686.

A data processor may decide: what IT systems or other methods to use to collect personal data; how to store the personal data; the detail of the security surrounding the personal data; the means used to transfer the personal data from one organisation to another; the means used to retrieve personal data about certain individuals; the method for ensuring a retention schedule is adhered to; and the means used to delete or dispose of the data.

29. *See infra* Part III.A.

30. MAYER-SCHÖNBERGER, *supra* note 4, at 137.

2. OECD Privacy Principles

The Organisation for Economic Co-operation and Development ("OECD")[31] introduced its proposal for internationally agreed upon privacy principles in the 1970s.[32] The OECD Privacy Principles were amended in July 2013 to "recognis[e] that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks."[33] The amended principles were also a response to the fact that "continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border cooperation among privacy enforcement authorities."[34] Neither the 1980 version nor the 2013 revision to the OECD Privacy Principles recognized a right of data subjects to be forgotten.[35] During the decades since the Principles were adopted, the fundamental nature of cross-border data flow has changed.[36]

3. The Charter of Fundamental Rights of the EU

The Charter of Fundamental Rights of the European Union ("the Charter"),[37] a founding document that memorializes fundamental rights enjoyed by all EU citizens, states that "human dignity is inviolable."[38] The European approach generally favors dignity-based pri-

---

31. The OECD "is a forum of countries committed to democracy and the market economy." *Organisation for Economic Co-operation and Development*, WIKIPEDIA, http://en.wikipedia.org/wiki/Organisation_for_Economic_Co-operation_and_Development (last visited Feb. 18, 2015). The organization provides a setting where governments "compare policy experiences, seek answers to common problems, identify good practices and coordinate domestic and international policies." *Id.*

32. *See* Ben Gerber, OECD PRIVACY PRINCIPLES, http://www.oecdprivacy.org (last visited Feb. 24, 2015).

33. ORG. FOR ECON. CO-OPERATION AND DEV. (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA ch. 1, 11 (1980) [hereinafter OECD, OECD PRIVACY GUIDELINES], *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

34. *Id.*

35. Rick Mitchell, *Revised OECD Privacy Guidelines Focus on Accountability, Notification of Breaches*, BLOOMBERG BNA (Sept. 16, 2013), http://www.bna.com/revised-oecd-privacy-n17179877087.

36. OECD, OECD PRIVACY GUIDELINES, *supra* note 33, ch. 2, at 29. "When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices. Services, such as 'cloud computing,' allow organisations and individuals to access data that may be stored anywhere in the world." *Id.*

37. Charter of Fundamental Rights of the European Union, 2010 O.J. (C 83) 389 [hereinafter Charter of Fundamental Rights], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

38. *Id.* art. 1, at 392.

vacy over the freedom of expression.[39] While Article 7 of the Charter focuses on general privacy protection for the individual,[40] Article 8 enshrines the protection of personal data as a fundamental right by imposing the same level of data protection throughout the EU.[41]

Nevertheless, the European right to protection of personal data is not absolute.[42] Protection of personally identifiable data is subject to other fundamental rights such as freedom of expression.[43] Article 11 of the Charter creates a freedom of expression that gives individuals the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[44] Article 8 of the European Convention of Human Rights ("ECHR") gives individuals a right to be respected in their personal life.[45] However, it acknowledges that the right to privacy must be balanced against other rights:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[46]

Additionally, Article 12 of the Universal Declaration of Human Rights ("UDHR") protects against interference with an individual's privacy, honor, and reputation,[47] but Article 19 nonetheless balances privacy against the "freedom of opinion and expression; this right includes freedom to hold opinions without interference."[48] Privacy in the Eurozone is an important value but must always be balanced against the freedom of expression.

---

39. *See* Donald C. Dowling Jr. & Jeremy M. Mittman, *International Privacy Law*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 403, 406 (Kristen J. Mathews ed., 2009).

40. Charter of Fundamental Rights, *supra* note 37, art. 7, at 393.

41. *Id.* art. 8, at 4.

42. Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen (Nov. 9, 2010) (striking a regulation that allows personal data on agricultural aid beneficiaries to be published without "drawing a distinction based on relevant criteria").

43. *See* Charter of Fundamental Rights, *supra* note 37, art. 52(1), at 402.

44. *Id.* art. 11(1), at 5.

45. ECHR, *supra* note 22, art. 8.

46. *Id.*

47. UDHR, *supra* note 22, art. 12, at 73–74.

48. *Id.* art. 19, at 74–75.

B. The Data Protection Directive of 1995

The current governing privacy law in the European Union is Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.[49] Directive 95/46/EC required each member state to pass national legislation that protects "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[50] The Directive required EU member states to pass national implementing legislation, which resulted in divergent data protection rules in different EU countries.[51]

The European Commission proposed the Directive because the data protection traditions at that time varied significantly across the member states. Germany, France, and the United Kingdom, for example, had relatively strong traditions of privacy protection, while Greece had no extant data protection policy.[52] In general, however, European privacy rights reflected respect for one's image, name, and reputation.[53] This dignity-based right originates from a concept in German constitutional law, *Informationelle Selbstbestimmung*, or informational self-determination,[54] which describes an individual's right to determine how they are portrayed to third parties and to the public.[55] The concept that the individual has a property interest in controlling information that relates to him or her is consistent with the concept that "knowledge about me is . . . my property."[56]

One of the Directive's prefatory clauses expressly states that the EU Commission enacted the Directive to protect fundamental rights including the right of privacy:

> Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the Europe-

---

49. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

50. *Id.* art. 1(1), at 38.

51. Douwe Korff, EC Study on Implementation of Data Protection Directive 47 (Sept. 2002) (unpublished study) (emphasis omitted), *available at* http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE ("All in all, the laws therefore vary considerably in the scope of the exceptions and in the tests applied (which are often quite vague).").

52. RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 187 (1st ed. 2002).

53. James Q. Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1153, 1161 (2004).

54. *See* Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 686–87 (1989).

55. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] June 3, 1980, 54 Entscheidungen des Bundesverfassungsgerichs [BVerfGE] 148 (155) (F.R.G.).

56. Hayden Ramsay, *Privacy, Privacies and Basic Needs*, HEYTHROP J. 288, 288 (2010).

> an Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.[57]

Directive 95/46/EC, which was drafted before the advent of the World Wide Web, included no express right to be forgotten.[58] However, in the recent ruling by the CJEU in *Google Spain v. AEPD*,[59] the court found an implied right to be forgotten in Directive 95/46/EC that triggered Google's duty to respond to takedown requests.[60]

1. Rights and Duties Under the Data Protection Directive

As its foundational principle, Directive 95/46/EC gives data subjects control over the collection, transmission, and use of personal information.[61] Under the Data Protection Directive, data processing is legal if the individual has given his unambiguous consent or one of several additional circumstances is met.[62] Article 7 of the Data Protection Directive states:

> Member States shall provide that personal data may be processed only if:
>
> (a) the data subject has unambiguously given his consent; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

57. Council Directive 95/46, *supra* note 49, at Preamble ¶ 10, at 32.

58. *See generally id.*

59. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

60. *Id.* ¶ 72, Ruling ¶ 1.

61. Personal data includes "any information relating to an identified or identifiable natural person" whether "by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Council Directive 95/46, *supra* note 49, art. 2(a), at 38.

62. *Id.* art. 7, at 40.

> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).[63]

Data subjects also have the right to obtain copies of information collected and the right to correct or delete personal data.[64] Companies must obtain consent from the data subject prior to entering into an agreement to share personally identifiable information.[65]

Companies may be held judicially liable for unlawfully processing personal data.[66] Regulators may also assess fines against companies that collect, process, or transmit information without obtaining a data subject's verifiable consent.[67] This is what occurred in *Union Fédérale des Consommateurs (UFC) v. AOL France*.[68] AOL France's standard contracts contained a clause that effectively stated the subscriber's personal data would be transferred outside the European Union and communicated to third-party direct marketers.[69] A French court ruled that a data subject's consent needs to be memorialized by a positive act.[70] The opt-out approach urged by AOL was too complex in requiring consumers to take too many steps.[71] If a U.S. company targets European consumers, they must comply with the consent requirements of the Data Protection Directive.

---

63. *Id.*
64. *Id.* art. 12, at 42.
65. *See id.* art. 7(b), at 40.
66. *Id.* art. 23, at 45.
67. David E. Dukes et al., *Don't Click "Send" Until You Read This: Protection of Privacy in International Data Transfers*, FOR THE DEF., Sept. 2010, at 68, 90 (2010).
68. *See B2C in Europe and Avoiding Contractual Liability: Why Businesses with European Operations Should Review Their Customer Contracts Now*, Morrison & Foerster (Aug. 5, 2004), http://www.mofo.com/resources/publications/2004/08/b2c-in-europe-and-avoiding-contractual-liability__.
69. *Id.*
70. *Id.* (stating that a positive act would mean for example "ticking a box expressing consent, rather than omitting to tick a box expressing objection").
71. *Id.*

2. Extraterritorial Effects of Directive 95/46/EC

European countries have often imposed regulations on the Internet that have extraterritorial effects on U.S. companies. Twitter, for example, obeyed a French court order to unveil anonymous anti-Semitic speakers using its service.[72] The International Federation of Human Rights ("FIDH") and the French League of Human Rights ("LDH") filed suit against the U.S. National Security Agency for its PRISM data collection program, as well as Internet companies such as Facebook and Skype, for violating the privacy rights of French citizens.[73]

The Data Protection Directive, too, has an extraterritorial impact on U.S. companies.[74] The Directive forbids the transfer of personal information across national borders unless the receiving country has implemented an adequate level of protection,[75] a requirement that threatens to halt the transfer of European personally identifiable data to the United States.[76] After Google negotiated in 2008 to reduce the retention period of personally identifiable data to eighteen months,[77] the Article 29 Working Party still found that Google was not in compliance with the Directive.[78] The consensus in the European Union "is

72. *Twitter Releases User Data to France After Lawsuit over Anti-Semitic Tweets*, JNS.ORG (July 12, 2013), http://www.jns.org/news-briefs/2013/7/12/twitter-releases-user-data-to-france-after-anti-semitic-tweets-lawsuit.

73. *France To Sue NSA? Rights Groups Urge Court To Open Lawsuit over US Spying*, RT (July 11, 2013), http://rt.com/news/french-sue-us-nsa-947. The French attorney representing the French human rights organizations contended, "We have never seen such an infringement on individual freedoms, to such a large scale, from a foreign nation and it potentially affects all French citizens and all French internet users when they use Google, Microsoft, Apple, Skype and other companies." *Id.*

74. *See, e.g.*, *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last updated Dec. 18, 2013) ("Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework's requirements . . . .").

75. Council Directive 95/46, *supra* note 49, art. 25, at 45–46; *id.* ("The European Commission's Directive on Data Protection . . . would prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) 'adequacy' standard for privacy protection.").

76. Mozelle W. Thompson, Comm'r, Fed. Trade Comm'n, *US/EU Safe Harbor Agreement: What It Is and What It Says About the Future of Cross Border Data Protection*, PRIVACY REG., Jan. 1, 2003, at 4–5, *available at* https://www.ftc.gov/public-statements/2003/01/useu-safe-harbor-agreement-what-it-what-it-says-about-future-cross-border ("Absent some agreement between the US and the EU, the Privacy Directive threatened to disrupt transatlantic commerce by blocking the ability of European organizations to transfer employee records, customer records and other types of personal data to companies in the United States.").

77. *See* Drake Bennett, *Stopping Google*, BOS. GLOBE (June 22, 2008), http://www.boston.com/bostonglobe/ideas/articles/2008/06/22/stopping_google/?page=full.

78. Press Release, Article 29 Data Prot. Working Party, *EU Data Protection Group Says Google, Microsoft and Yahoo! Do Not Comply with Data Protection Rules* (May 26, 2010), http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_05_10_en.pdf. The Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal

that the United States lacks an adequate level of protection."[79] The GDPR's expansive right to be forgotten creates the potential to further impede data flow from EU countries to the United States and threaten e-commerce.[80]

C. Google Spain v. AEPD

1. Facts

Google Spain v. AEPD[81] is a bellwether decision by the Court of Justice of the European Union that recognized a right to be forgotten under the Data Protection Directive.[82] In 2010, Mario Costeja González, a Spanish national, filed a complaint with the Spanish Data Protection Agency ("Agencia Española de Protección de Datos", "AEPD") against La Vanguardia Ediciones SL, a large publisher of daily news in Spain, as well as Google Spain and Google Inc.[83] González, the data subject seeking erasure, contended that when Internet users entered his name in a Google search, the results linked to *La Vanguardia* newspaper articles containing announcements for a real-estate auction related to attachment proceedings that began after González failed to pay social security debts.[84] He contended that the articles, "although truthful, injured his reputation and invaded his privacy."[85] González demanded that the Spanish newspaper erase them because they were no longer relevant, since the proceedings had concluded more than a decade ago.[86] The newspaper publisher refused to erase the articles because the Ministry of Labour and Social Affairs had ordered their publication.[87] Next, the plaintiff demanded that

---

Data is "an independent advisory body on data protection and privacy . . . . set up under Article 29 of the Data Protection Directive 95/46/EC." *Id.*

79. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1968, 1980 (2013).

80. *Cf.* Viviane Reding, Vice-President of the Eur. Comm'n and EU Justice Comm'r, Speech at the New Frontiers for Social Media Marketing Economist Conference (Nov. 29, 2011), *in EU Data Protection Reform and Social Media: Encouraging Citizens' Trust and Creating New Opportunities*, EUR. COMMISSION, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/827&type=HTML (last modified February 12, 2015).

81. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

82. *Id.* at Ruling ¶¶ 1–4.

83. *Id.* ¶ 14.

84. *Id.*

85. Dave Lee, *What Is the "Right To Be Forgotten"?*, BBC (May 13, 2014), http://www.bbc.com/news/technology-27394751.

86. *Google Spain SL*, Case C-131/12, ¶ 15.

87. Opinion of Advocate General Jääskinen ¶ 19, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014) (Case C-131/12), http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&doclang=EN.

Google remove the link to those stories and thereby eliminate any association to his name.[88]

2. Procedural History of *Google Spain v. AEPD*

The AEPD ruled that Google was responsible as a data controller for removing results about the plaintiff from its search engine.[89] After the AEPD's decision, Google brought action before the Audiencia Nacional, Spain's highest court, which referred the case to the Court of Justice of the European Union.[90] On June 25, 2013, Advocate General Niilo Jääskinen issued his advisory opinion, finding that Google had no responsibility to remove any links on its search engine based on a privacy claim.[91] He reasoned that suppressing legitimate and legal information already in the public domain would interfere with freedom of expression and undermine the objectivity of information on the Internet.[92]

The CJEU rejected the Advocate General's argument and recognized a broad right to be forgotten under Spain's implementation of Directive 95/46/EC.[93] The court found that Google, as an indexer of information, was processing personal data and therefore subject to the Directive's obligations for data controllers.[94] The court drew upon Articles 12(b)[95] and 14(a)[96] of the Directive to hold that Google owed a duty to erase information from its search index.[97] The CJEU rejected Google's argument that imposing a duty to remove personal data violated the principle of proportionality, and that such removal must be addressed to the publisher of the website because the publisher was responsible for making the information public.[98] The court reasoned that search engines make access to this information effortlessly available, because they enable users to obtain information about a data

88. *Id.*

89. *Google Spain SL*, Case C-131/12, ¶ 17.

90. *Id.* ¶¶ 18–20.

91. Opinion of Advocate General Jääskinen, *supra* note 87, ¶ 138.

92. *Id.* ¶¶ 120–34.

93. *Google Spain SL*, Case C-131/12.

94. *Id.* ¶ 41.

95. Council Directive 95/46, *supra* note 49, art. 12(b), at 42 (stating that the data subject shall have a right to obtain from the controller "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 and inaccurate nature of the data").

96. *Id.* art. 14(a), at 42 (stating that the data subject has a right to object "at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him").

97. *Google Spain SL*, Case C-131/12, ¶ 82.

98. *Id.* ¶ 63. Google also argued that the least cost avoider for removing access to the information was the website and not the search engine. They argued that to require a search engine to remove content from its index "would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of the operator itself." *Id.*

subject by simply typing the subject's name.[99] Due to their preeminent role in organizing data, search engines like Google are far more likely to interfere with the data subject's right to privacy than the original website publisher.[100]

3. Pitfalls of *Google Spain v. AEPD*

After *Google Spain v. AEPD*, data subjects in Europe gained a right to demand that Google delete links to websites that appear when searching for their names unless there are legitimate reasons not to remove them,[101] even if the original website has not taken down the content and the data is truthful and otherwise lawful.[102] However, the original information about González will not be scrubbed from the Internet; it is only removed from a Google search of his name.[103] Thus, requiring a search engine to provide Internet users with a right to be forgotten is not about deleting or forgetting content, but making it more difficult to locate.[104] Further, Google may not be technically eliminating the connection between the data subject and the published information because the deleted link could still be available in Google's backup files. Indeed, links that Google removes from EU search results will remain in searches made from non-EU domains.[105]

---

99. *Google Spain SL*, Case C-131/12, ¶ 80.

100. *Id.* ¶ 87.

101. *Id.* ¶ 94. According to the decision, Google has to examine each request on the merits, and no algorithm or automatized procedure has been used so far to process requests. Press Release, Eur. Court of Justice of the Eur. Union, 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; Joe Silver, *Google Inundated with "Right To Be Forgotten" Requests*, ARS TECHNICA (June 2, 2014), http://arstechnica.com/tech-policy/2014/06/google-inundated-with-right-to-be-forgotten-requests/.

102. *Google Spain SL*, Case C-131/12, ¶ 94.

103. Rich Trenholm, *Google Must Delete Search Results on Request, Rules EU Court*, CNET (May 13, 2014), http://www.cnet.com/news/google-must-delete-search-results-rules-european-court (quoting Bill Echikson, Google's Head of Free Expression, who noted that "only the original publisher can take the decision to remove such content" and "[o]nce removed from the source webpage, content will disappear from a search engine's index").

104. Peter Fleischer, *"The Right To Be Forgotten", Seen from Spain*, PETER FLEISCHER: PRIVACY...? (Sept. 5, 2011), http://peterfleischer.blogspot.se/2011/09/right-to-be-forgotten-seen-from-spain.html; *see also* David Drummond, *We Need to Talk About the Right To Be Forgotten*, GUARDIAN (July 10, 2014), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate ("The Guardian could have an article on its website about an individual that's perfectly legal, but we might not legally be able to show links to it in our results when you search for that person's name. It's a bit like saying the book can stay in the library but cannot be included in the library's card catalogue.").

105. Vlad Tiganasu, *Google Keeps Its Limitations on "Right To Be Forgotten" Requests*, ARTICLES INFORMER (Feb. 2015), http://articles.informer.com/google-keeps-its-limitations-on-right-to-be-forgotten-requests.html.

Erasing social media posts that have gone viral is akin to attempting to hold back the ocean with a single whiskbroom.

In the debate over the right to be forgotten, the sole focus on Google is also misplaced as there are numerous other search engines.[106] Critics from the House of Lords in the United Kingdom emphasize that the CJEU did not consider the ruling's effect on smaller search engines, which are "unlikely to have the resources to process thousands of removal requests."[107] Furthermore, they argue that it is "'wrong in principle' to leave it to search engines to decide whether or not to delete information, based on 'vague, ambiguous and unhelpful' criteria."[108]

D. The General Data Protection Regulation

In January 2012, the European Commission proposed the GDPR.[109] The main purpose of the Data Protection Regulation[110] is to update data protections in light of the rapid technological changes that have taken place since Directive 95/46/EC entered into force in 1995.[111] The GDPR, which explicitly recognizes a right to be forgot-

---

106. For example, Microsoft's Bing recently released its takedown form in response to *Google Spain v. AEPD*. *See* Microsoft, *Request To Block Bing Search Results in Europe*, BING, https://www.bing.com/webmaster/tools/eu-privacy-request (last visited July 21, 2014).

107. Catherine Baksi, *Right To Be Forgotten "Must Go", Lords Committee Says*, LAW GAZETTE (July 30, 2014), http://www.lawgazette.co.uk/law/right-to-be-forgotten-must-go-lords-committee-says/5042439.fullarticle.

108. *Id.*

109. *GDPR*, *supra* note 15. The Data Protection Regulation and "a separate Data Protection Directive[] covering the 'processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'" will replace the current Directive 95/46/EC. PAUL BERNAL, INTERNET PRIVACY RIGHTS: RIGHTS TO PROTECT AUTONOMY 93 (2014) (noting that the separate directive "allow[s] greater leeway for governments").

110. A European regulation is a legal instrument binding in all of its parts. More importantly, it is self-executing, which means that it is immediately enforceable as law in all member states. In contrast, a European directive is not self-executing, and while it is binding on the member states as to the ultimate result, it leaves to individual countries the choice of the form and method they adopt to realize the Union objectives within the framework of their internal legal order. *See Regulations, Directives and Other Acts*, EUROPA, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm (last visited Feb. 17, 2015). Furthermore, a regulation results in more harmony because all EU countries must follow its precise terms. By contrast, a directive is more flexible because it requires member states to meet just a certain minimum standard, but member states can improve that minimum with more stringent provisions. *See* U.S. Dep't of Agric., *Difference Between a Regulation, Directive and Decision*, USDA FOREIGN AGRIC. SERVICE, http://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision (last modified Dec. 7, 2014).

111. *GDPR*, *supra* note 15, at Explanatory Memorandum § 1, at 1. The European Commission describes the GDPR as introducing "three main innovations . . . a single, pan-European law for data protection . . . a 'one-stop-shop' for businesses . . . [and] [t]he same rules for all companies — regardless of their establishment." Press Release, Eur. Comm'n,

ten that applies not only to search engines but also to source websites and other data controllers, was introduced by the European Commission in January 2012 and approved by the Civil Liberties, Justice and Home Affairs Committee of the European Parliament ("LIBE").[112] The EU Parliament approved the GDPR, which will supersede Directive 95/46/EC when it enters into force in 2017.[113] The next step is to initiate the trilogue procedure where the EU Commission, Parliament, and Council "will try to agree upon the final form of the Regulation."[114]

The GDPR consists of a single regulation focusing on the privacy protection of users, along with a directive which aims to prevent, detect, investigate, or prosecute criminal offenses, and further related judicial activities.[115] The GDPR has two main objectives: to enhance individuals' control over their personal data, and to provide legal certainty to and minimize administrative burdens for businesses.[116] The newly minted regulation aims to set data protection rules that operate across Europe, since the application of disparate standards to nationals and non-nationals is antithetical to an open Internet.[117]

1. An Anatomy of the GDPR's Right To Be Forgotten

The right to be forgotten can be conceptualized as taking three forms: (1) the right to have information deleted after a preset period; (2) the right to have a clean slate; and (3) the right to be connected to current information and delinked from outdated information.[118] The first form of the "right to be forgotten" is the right for data subjects to require other individuals or organizations to erase information about them, and this applies whether it is the data subject or a third party

---

Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014), http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

112. Viviane Reding, Vice-President of the Eur. Comm'n and EU Justice Comm'r, Speech at the Centre for European Policy Studies (Jan. 28, 2014), *in Data Protection Compact for Europe*, EUROPEAN COMM'N, http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm; Press Release, Eur. Comm'n, LIBE Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013), http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

113. Press Release, Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote, *supra* note 111; Foster, *supra* note 21.

114. Foster, *supra* note 21.

115. Press Release, Eur. Comm'n, Data Protection Day 2014: Full Speed on EU Data Protection Reform (Jan. 27, 2014) [hereinafter Eur. Comm'n, Data Protection Day], http://europa.eu/rapid/press-release_MEMO-14-60_en.htm.

116. Hans Graux et al., *The Right To Be Forgotten in the Internet Era* 12 (Interdisciplinary Ctr. for Law & ICT, Univ. of Leuven, Working Paper, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2174896.

117. *See* Reding, Speech at the New Frontiers for Social Media Marketing Economist Conference, *supra* note 80.

118. *See* Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice*, 8 SCRIPTED 229, 236 (2011).

who has posted the information.[119] The second and third conceptualizations are similar because they both provide a possibility for a fresh start — the right to slip up and to evolve by learning from mistakes, and the right to keep information up-to-date, respectively.[120] These latter two versions of the right to be forgotten would allow people to "shape their own lives," while the first lets other people do it for them.[121]

Article 17 of the GDPR gives data subjects in the twenty-eight countries of the European Union a right to be forgotten. Article 17 establishes a methodology for determining when a data subject can exercise the right of erasure, data controllers' obligation to erase links to third-party websites, and how to exercise that right.[122] A data subject has the right to erase links to data relating to him or her if the information is:

> no longer necessary in relation to the purposes for which [it was] collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation.[123]

The right of erasure applies equally to private persons, public officials, and public figures such as celebrities.[124] The right of erasure is not absolute, as Article 17(3) makes this right subject to free expression online and a data controller's right to obtain personal data for reasons of historical, statistical, public health, and scientific research

---

119. *Id.* at 237.

120. *See generally* Jean-François Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 INFO. SOC'Y 33 (1998) (discussing the importance of social forgetfulness); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 229 (2008) (proposing a voluntary reputational bankruptcy to get a fresh start to counter the permanence of digital footprints).

121. Koops, *supra* note 118, at 236.

122. *GDPR*, *supra* note 15, art. 17(1), 17(3), at 51–53*; see also* Kate Brimsted, *The Right To Be Forgotten: Can Legislation Put the Data Genie Back in the Bottle?*, 11 PRIVACY & DATA PROT. 6, 7 (2011).

123. *GDPR*, *supra* note 15, at Preamble ¶ 53, at 25. The most defensible right of erasure applies to personal data collected while a data subject was a child and which is no longer relevant. Here, the child is not likely to be cognizant "of the risks involved by the processing, and later wants to remove such personal data especially on the Internet." *Id.*

124. *See id.* art. 14(1), at 41 ("'[D]ata subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.").

purposes.[125] These statutory carve-outs and exceptions to the right to be forgotten are discussed in more detail below.[126]

The EU Commission does not indicate how data controllers are to determine when data that is the subject of an erasure request is no longer necessary or where there is no legal basis for retaining it, so the burden falls on the data controller to determine those factors.[127] The following hypothetical illustrates the difficulty of making those decisions:

> For instance, consider a photograph depicting Alice and Bob engaged in some activity at a given time and place. Suppose Alice wishes the photo to be forgotten, while Bob insists that it persist. Whose wishes should be respected? What if multiple people appear in a group photo? Who gets to decide if and when the photo should be forgotten? In another example, Bob incorporates part of a tweet he receives from Alice into a longer blog post of his own. When Alice later exercises her right to remove her tweet, what effect does this have on the status of Bob's blog post? Does Bob have to remove his entire blog post? Does he have to remove Alice's tweet from it and rewrite his post accordingly? What criteria should be used to decide?[128]

Nor does the EU right to be forgotten proposal distinguish between true or false information,[129] so data subjects will also be able to suppress truthful information as long as the data does not fit within a statutory exception. This places the data controller in the unenviable position of effectively rewriting history. Furthermore, data controllers must make these decisions in a vacuum. The right of erasure, as articulated in the GDPR, does not impose a burden on data subjects to provide any factual foundation for their data request or even assert that the website posting or other information that is the basis for the request violates the law, defames, or humiliates.[130] The consequence of the broad right of erasure is that Google and other data controllers are in the position of gatekeepers that determine which data erasure

---

125. *Id.* art. 17(3), at 52.

126. *See infra* Part II.D.3.

127. *See GDPR*, *supra* note 15, art. 17(1)(a), at 51.

128. PETER DRUSCHEL ET AL., EUR. NETWORK AND INFO. SEC. AGENCY (ENISA), THE RIGHT TO BE FORGOTTEN — BETWEEN EXPECTATIONS AND PRACTICE 7 (2011), https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport.

129. *See GDPR*, *supra* note 15, art. 17, at 51–53, art. 4(2), at 41.

130. *See id.* art. 17, at 51–53.

requests should be granted and which should be denied, without sufficient guidance.[131]

2. Duties of Data Controllers

The EU Commission's Explanatory Memorandum makes a policy-based decision that the data controller, not the data subject, must notify third-party websites that a data subject has requested that it "erase any links to, or copy or replication of . . . personal data."[132] The Memorandum treats the data controller as an intermediary between the data subject and third-party websites that originally published the personal data at issue.[133] The Data Protection Regulation imposes an indeterminate reasonableness standard for data controllers to take all steps, including employing technical measures, to inform third parties of data removal requests.[134] Data controllers face "ruinous monetary sanctions" if they "'do[] not comply with the right to be forgotten or to erasure' — a fine up to 1,000,000 euros or up to two percent of Facebook's annual worldwide income."[135] Restoring the balance be-

131. Two months following the *Google Spain v. AEPD* decision, Google appointed an advisory committee to help it determine the balance between takedown demands and the public's right to know. *See* Natasha Lomas, *Google Seeks To Shape Public Debate on Europe's Right To Be Forgotten Ruling*, TECHCRUNCH (July 11, 2014), http://techcrunch.com/2014/07/11/google-agitates-for-public-debate-on-europes-right-to-be-forgotten-ruling.

132. *GDPR*, *supra* note 15, art. 17(2), at 51.

133. *See id.* (requiring data controllers to take all reasonable steps to inform third parties that are processing data that is subject to the removal request that a data subject has requested removal).

134. *See id.* Article 17(2) states, "Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data." *Id.* Academic commentators caution that the proposed Regulation's vague admonitions create boundless liability for data controllers:

> The vagueness of a generic obligation to take "all reasonable steps . . . to inform" third parties when such a right is exercised is worrisome, particularly because of the Regulation's new, sterner penalties. Similarly, the simple statement that data controllers "shall be considered responsible" for the publication of personal data by a third party, when they have authorized it at the end of the second paragraph, belies the complexity of the underlying mechanisms. When will a publication be "authorized?" And what precisely does being "responsible" entail in terms of duties or liabilities? On these points, the current draft of the regulation leaves a great deal open to interpretation.

Meg L. Ambrose & Jef Ausloos, *The Right To Be Forgotten Across the Pond*, 3 J. INFO. POL'Y 1, 12 (2013).

135. Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90–91 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf.

tween data subject and data controller "has long been debated in Europe" and is the impetus behind a right to be forgotten.[136]

3. Exceptions to the Data Protection Regulation

The data controller is not required to initiate erasure if the subject of the data request falls into one of Article 17(3)'s four statutory carve-outs, one exception to accommodate expression and three others which recognize the public's right to know:

> (a) for exercising the right of freedom of expression in accordance with Article 80;
>
> (b) for reasons of public interest in the area of public health in accordance with Article 81;
>
> (c) for historical, statistical and scientific research purposes in accordance with Article 83;
>
> (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued[137]

The EU Commission does not provide data controllers with a template for determining whether a given data request collides with the freedom of expression.[138] Other sources of EU law flesh out the contours and limitations of expression, but these are broad standards, not the bright-line rules needed by data controllers that must process hundreds of thousands of data requests per year. Article 11 of the Charter, which corresponds to Article 10 of the ECHR, states that European citizens have a broad freedom of expression that includes the freedom to hold opinions and to receive and impart information and ideas without the interference of a public authority.[139] The EU's freedom of expression encompasses not only the freedom of speech and information but also guaranteed access to the public.[140] However, the freedom of expression is not absolute; it does not include a right to defame or to use speech to threaten public safety, national security,

136. 3 ELENI KOSTA, CONSENT IN EUROPEAN DATA PROTECTION 252 (Fabian Amtenbrink & Ramses A. Wessel eds., 2013).

137. *GDPR*, *supra* note 15, art. 17(3), at 51.

138. *See id.* art. 17(3)(a), at 51.

139. Charter of Fundamental Rights, *supra* note 37, art. 11(1), at 394.

140. *See* PETER BLUME, PROTECTION OF INFORMATIONAL PRIVACY 140–41 (2002).

crime prevention, the protection of health and morals, the prevention of disclosure of information received in confidence, and the authority and impartiality of the judiciary.[141]

The European Commission also provides little guidance on how to respond to data requests to accommodate the policy interest in public health.[142] Similarly, it is unclear how data controllers should determine what data requests are important for historical, statistical, or scientific purposes.[143] Finally, Article 17(3) articulates a general standard that data controllers can retain personal data if retention accords with EU or member state law, which inevitably requires balancing a data subject's request against the public interest, "respect[ing] the essence" of the right to data protection, and remaining "proportionate to the legitimate aim pursued."[144] However, the Commission does not formulate a template for how search engines should weigh or balance these factors in making the decision to grant or reject a data subject's demand to delink.

E. Negative Consequences of the GDPR's Right To Be Forgotten

1. The GDPR and Censorship

In the aftermath of the *Google Spain v. AEPD* case, data controllers have removed links to a number of newsworthy items. Some examples of link removals have become public because Google notified media outlets such as *BBC* and *The Guardian* when it removed their respective stories from search results.[145] That prompted critics to charge that Europe's Internet was being scrubbed and its press was being censored.[146] In order to protest the link removals, Wikimedia Foundation, a nonprofit that operates the online encyclopedia Wikipedia, decided to post all link removal notices that it receives to "attract[] attention to the very information someone wanted removed."[147]

---

141. ECHR, *supra* note 22, art. 10; *see also* Explanations Relating to the Charter of Fundamental Rights, Explanation on Article 11 — Freedom of Expression and Information, 2007 O.J. (C 303) 17, 21, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007X1214(01)&from=EN.

142. *See GDPR*, *supra* note 15, art. 17(3)(b), at 52.

143. *See id.* art. 17(3)(c), at 51.

144. *See id.* art. 17(3)(d), at 51.

145. *See* Araminta Wordsworth, *EU's Right To Be Forgotten Ruling a New Name for Censorship*, NAT'L POST (Sept. 9, 2014), *available at* https://web.archive.org/web/20140911121125/http://fullcomment.nationalpost.com/2014/09/09/eus-right-to-be-forgotten-ruling-a-new-name-for-censorship.

146. *Id.*

147. *Id.*; *Notices Received from Search Engines*, WIKIPEDIA, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last modified Nov. 27, 2014); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA BLOG (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results.

An overly expansive right to be forgotten will lead to censorship of the Internet because data subjects can force search engines or websites to erase personal data, which may rewrite history.[148] Other commentators contend that if content becomes less searchable on the Internet, it will "derogate[] the role of counterspeech" and "disrupt the natural process of communication."[149] The right to be forgotten should not subordinate the freedom of expression because free and open public access enables citizens to discuss and share information about society.[150] A right to be forgotten would "deny the would-be speaker the ability to decide what to say and think, and deny the would-be listener the information desired to form his opinions and ideas."[151]

Advocates of a right to be forgotten argue that the GDPR will strengthen already existing privacy rights.[152] An EU official involved in the development of the GDPR proposal has stressed that "freedom of expression is not a good argument for not having a right to be forgotten."[153] There is also a concern that too much deference to free expression will cannibalize the right to privacy. However, similar to Directive 95/46/EC, the GDPR strives to balance these rights by presenting freedom of expression as a limitation on the right to delete.[154] According to Article 80(2) of the GDPR, it is up to each member state to more specifically determine what to include in the freedom of expression exception within two years after the GDPR enters into force.[155] In addition, member states must provide their citizens with a right to freedom of expression, which is a fundamental right for all citizens of the EU.[156]

2. The GDPR and the Chilling Effect on Journalists

Journalists are concerned that a right to be forgotten will delay investigations and create gaps in stories as a result of search engines

148. *See* David Mitchell, *The Right To Be Forgotten Will Turn the Internet into a Work of Fiction*, OBSERVER (July 5, 2014), http://www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google (describing takedown requests that include "a British politician who's trying to make a comeback, someone convicted of possessing child abuse images and a doctor who doesn't want negative reviews from patients to be searchable").

149. Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right To Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. & POL'Y 91, 114 (2013).

150. *See id.*

151. *Id.* at 119.

152. *See, e.g.*, Eur. Comm'n, Data Protection Day, *supra* note 115, at 3.

153. Telephone Interview with EU official involved with the drafting of the GDPR (Dec. 11, 2012) (name and title withheld at interviewee's request).

154. *See GDPR*, *supra* note 15, art. 17(3)(a), at 52.

155. *Id.* art. 80(2), at 94–95, art. 91(2), at 99.

156. Charter of Fundamental Rights, *supra* note 37, art. 11, at 394.

removing indispensable data.[157] Article 9 of Directive 95/46/EC provides for an exception from deletion for "journalistic purposes or the purpose of artistic or literary expression."[158] At present, there is uncertainty as to how this provision should be interpreted and whether it effectively protects journalists and the information they post online.[159] The court's decision in *Google Spain v. AEPD* found that the Data Protection Directive included a right to be forgotten even though it contained no express provision giving a right to delete.[160] The decision of the CJEU did not require the search engine to delete the postings themselves from the Internet.[161] After Google approves a takedown request, the requestor's name and other personal information would still exist on other web pages, which would not lead to any actual "forgetting" of such information. However, with the advent of the GDPR, data subjects might attempt to push the envelope further and request that websites delete the information itself, in addition to requesting that search engines decouple links. Such developments pose threats to journalism, as explained by the following example:

> After serving their sentences, convicted murderers Wolfgang Werlé and Manfred Lauber successfully invoked the German "right of rehabilitation" to pressure a number of German publications to scrub their names from online articles about their victim, actor Walter Sedlmayr. One news entity successfully challenged restrictions on their reporting, but for many German news organizations, it was already too late . . . . One such article explains: "In response to a cease-and-desist letter, the Süddeutsche Zeitung entered into an agreement not to publish the names of

157. *See* Mattias Goldmann & Jacob Dexe, *Låt Inte de Digitala Fotspåren Få Suddas Ut*, SVD OPINION (May 17, 2014), http://www.svd.se/opinion/brannpunkt/lat-inte-de-digitala-fotsparen-fa-suddas-ut_3568578.svd; *see also* Neil Brady, *Does the "Right of Erasure" Pose a Bigger Threat than the "Right To Be Forgotten"?*, GUARDIAN (July 10, 2014), http://www.theguardian.com/media-network/media-network-blog/2014/jul/10/right-forgotten-google-data-protection (quoting Irish solicitor) (arguing that the *Google Spain* decision "poses a threat to news dissemination in Europe, if not freedom of expression").

158. Council Directive 95/46, *supra* note 49, art. 9, at 41 ("Member States shall provide for exemptions or derogations from the provisions . . . for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.").

159. *See Data Protection Reforms Will Not Alter Journalists' Rights to Use of Personal Data*, OUT-LAW.COM (July 23, 2014), http://www.out-law.com/en/articles/2014/july/data-protection-reforms-will-not-alter-journalists-rights-to-use-of-personal-data.

160. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Ruling ¶¶ 1–4 (May 13, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

161. *See id.*

> the two convicted murderers in any future news report. This also applies to user comments . . . ."[162]

The GDPR has several safeguards to balance journalistic expression and privacy. Article 80 states that "Member States shall provide for exemptions or derogations from [Article 17] . . . for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression."[163] Recital 121 of the Preamble clarifies the intended scope of application:

> This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights . . . . Member States should classify activities as "journalistic" . . . if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.[164]

However, the European Commission has yet to define who qualifies as a journalist entitled to statutory protection. While traditional media such as newspapers, magazines, and traditional journalistic institutions are covered, it is unclear whether bloggers and other Internet commentators would also fall within the sphere of application of the journalistic exception.[165] In the age of the global Internet and the ubiquity of bloggers, tweeters, and microbloggers, anyone can

---

162. Katharine Larsen, *Europe's "Right To Be Forgotten" Regulation May Restrict Free Speech*, 17 FIRST AMENDMENT & MEDIA LITIG. 1, 13 (2013).

163. *GDPR*, *supra* note 15, art. 80, at 94–95.

164. *Id.* at Preamble ¶ 121, at 35–36.

165. *See* Council of the Eur. Union, 12274/2/14 REV 2, 1, 27, *available at* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012274%202014%20REV%202; Council of the Eur. Union, 11289/1/14 REV 1, 1, 11 nn.14–15, *available at* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011289%202014%20REV%201; Steve Peers, *"The Right To Be Forgotten": The Future EU Legislation Takes Shape*, EU L. ANALYSIS (Sept. 23, 2014), http://eulawanalysis.blogspot.com/2014/09/the-right-to-be-forgotten-future-eu.html.

express himself or herself in a journalistic fashion, or at least in an artistic or literary fashion.[166]

On the other hand, one risk is that courts will stretch the journalistic exception too far, since the purpose of every public disclosure is to spread information, opinions, or ideas. Such a broad interpretation of the journalism exception would swallow up the right to be forgotten. It is inconceivable that the European Commission dedicated 119 pages to the creation of rights only to take it away by a two-paragraph journalistic exception in Article 17(3).

Another concern is that the right to delete may vary depending on the EU member state and the arbitrary factor of where a data subject's keyboard happens to be located. Comments may be subject to removal in one country but not in another, a result inimical to EU harmonization. This further complicates an issue that is already a problem within the EU. When considering the question of whether the right to be forgotten should be expanded beyond Europe, different standards for removal are inevitable absent an international agreement.

III. THE TRANSATLANTIC CLASH: THE U.S. PERSPECTIVE

Due to the global nature of the Internet and the fact that American websites, social media websites, and search engines are using and processing the personal data of European users, this part of the Article examines the extraterritorial impacts on the right to be forgotten by comparing the U.S. legal system's treatment of privacy and freedom of expression. After the decision in *Google Spain v. AEPD*, the links that may be taken down from European search results "remain visible on Google.com, the U.S. version of the site."[167] Google's role in taking down content is emblematic of conflicting privacy rules on each side of the Atlantic.

A. U.S. Sectorial Approach to Consumer Privacy

The law of privacy in the United States is a patchwork of legislation, regulation, and self-regulation. The federal Privacy Act of 1974 only applies to the processing of information by federal agencies,[168] and the United States presently recognizes no general right to information privacy for information outside the sphere of the federal gov-

166. U.S. courts have ruled that bloggers are not journalists for the purposes of the First Amendment. *See, e.g.*, Obsidian Fin. Grp. v. Cox, 812 F. Supp. 2d 1220, 1234 (D. Or. 2011) *aff'd*, 740 F.3d 1284 (9th Cir. 2014).

167. AGENCE FRANCE PRESSE, *Google Is Having Trouble Determining the Legitimacy of Europe's 91,000 "Right To Be Forgotten" Requests*, BUS. INSIDER (Aug. 1, 2014), http://www.businessinsider.com/google-is-having-trouble-determining-the-legitimacy-of-europes-91000-right-to-be-forgotten-requests-2014-8.

168. Privacy Act of 1974, 5 U.S.C. § 552(b)–(f) (2010).

ernment.[169] The United States has no comprehensive privacy framework, but rather it legislates privacy rights by sector such as with the Health Insurance Portability and Accountability Act ("HIPAA"),[170] the Health Information Technology for Economic and Clinical Health Act ("HITECH"),[171] and the Gramm-Leach-Bliley Act ("GLBA").[172] This patchwork quilt of privacy protection often leads to uncertainty and confusion among the citizens regarding what rights they may enjoy and under what conditions they may act upon such rights.[173]

B. Aspirational Consumer Privacy Bill of Rights

While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States has only made limited attempts to enact comprehensive protection to align its privacy law with EU regulations. Shortly after the European Commission released its proposal to the GDPR, the White House released its own largely aspirational proposal, the Consumer Privacy Bill of Rights.[174] Similar to the GDPR, it aims to strengthen privacy protection for online users to create trust in the online environment, which will stimulate economic growth and innovation.[175] Drawn in large part from the OECD principles, it provides for the following core principles:

---

169. Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 273 (2008).

170. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

171. Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 115 (codified as amended at 42 U.S.C. §§ 17937, 17954 (2012)).

172. Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999) (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended at 15 U.S.C. § 6801 (2012)).

173. *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 67 (2004).

174. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; *see also* Press Release, Office of the Press Sec'y, The White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" To Protect Consumers Online (Feb. 23, 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

175. Office of the Press Sec'y, The White House, *supra* note 174. United States Secretary of Commerce John E. Bryson noted,

> Every day, millions of Americans shop, sell, bank, learn, talk and work online. At the turn of the century, online retail sales were around $20 billion in the United States, now they're nearing $200 billion . . . . The Internet has become an engine of innovation, business growth, and job creation, so we need a strong foundation of clear protections for consumers, and a set of basic principles to help businesses guide their privacy and policy decisions. This privacy blueprint will do just that.

Id.

> Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
>
> Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
>
> Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
>
> Security: Consumers have a right to secure and responsible handling of personal data.
>
> Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
>
> Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
>
> Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[176]

The Obama Administration seeks to improve global interoperability between the U.S. consumer data privacy framework and other countries' frameworks through mutual recognition, the development of codes of conduct through multi-stakeholder processes, and enforcement cooperation.[177] If Congress enacts this proposed statute, it will be a modest first step to harmonizing U.S. privacy law with European "mutually recognized privacy protection."[178] The Obama Administration also encourages Congress to provide strong authority to the Federal Trade Commission to make sure that online companies

176. *See* THE WHITE HOUSE, *supra* note 174, at 1.
177. *Id.* at 2–3.
178. *See id.* at 32.

abide by their privacy-related public promises.[179] However, President Obama's Consumer Privacy Bill of Rights does not contain an express or implied right to be forgotten.[180]

C. The Restrictive Right To Be Forgotten Under U.S. Law

Since the Consumer Privacy Bill of Rights does not contain any right to be forgotten provision, it is of great importance to look at the right to be forgotten in other contexts under U.S. law. Unlike in Europe, the right to be forgotten is undeveloped in the United States in large part because of the hegemony of the First Amendment.[181] However, several states have taken some modest first steps towards such a right.

1. Right of Expungement for Juvenile Offenses

The expungement of juvenile offenses is treated differently under statutory provisions than offenses committed when the defendant is an adult.[182] U.S. states generally provide for a right of juvenile offenders to file a petition in court to expunge a juvenile court conviction.[183] This sealing of the criminal history of an individual allows offenders to tell prospective employers, property owners, or licensing agencies that they have never been arrested or convicted.[184] The Florida legislature, for example, adopted a statute for the judicial sealing or expunction of a juvenile criminal history record for misdemeanors prior to July 1, 1996, although this option is not available if the juvenile was tried as an adult.[185] Although expungement laws typically only apply to juvenile offenders, some states extend the sealing of court records

---

179. *Id.* at 2.

180. *See generally id.*

181. *See* Larson, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right To Be Forgotten Are Incompatible with Free Speech*, *supra* note 149, at 92–93 (arguing that the right to be forgotten is incompatible with the First Amendment); *see also* Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 423–24 (2013) ("Though well-intentioned, the Eraser Button concept — like the 'right to be forgotten' — raises clear First Amendment issues by limiting the right of others to speak freely or to collect, analyze, or redistribute information they find online.").

182. James L. Buchwalter, *Cause of Action To Expunge Adult Record*, *in* 37 CAUSES OF ACTION 615 (2d ed. 2008).

183. DONALD T. KRAMER, 2 LEGAL RIGHTS OF CHILDREN § 23:18 (2d ed. 2005) ("[M]ost state codes provide some procedure by which these records can be destroyed, expunged, sealed, or otherwise made permanently inaccessible.").

184. *See, e.g.*, Greater Boston Legal Services, *Know Your CORI Rights*, MASSLEGALHELP, http://www.masslegalhelp.org/cori/booklets-folder/know-your-cori-rights.pdf (last updated Aug. 28, 2014).

185. Fla. Dep't of Law Enforcement, *Frequently Asked Questions*, FLA. DEPARTMENT OF L. ENFORCEMENT, http://www.fdle.state.fl.us/content/seal-and-expunge-process/menu/frequently-asked-questions.aspx#Record_Seales_or_Expunged.

to young adults.[186] The court in *In re Expungement for Spencer* stated that North Carolina's expungement statute did not accord the trial court discretion to order erasure of a criminal record of a person over twenty-one years of age.[187] The rules for the expungement of juvenile offenses vary between the states.

2. California's Right To Be Forgotten for Children

In September 2013, California passed Senate Bill No. 568,[188] which recognized a more limited right to be forgotten than Article 17 of the GDPR. When the California statute went into effect on January 1, 2015, it gave children a right to delete posts that they made to social media websites such as Facebook.[189] However, this narrow right of erasure will merely cover deletion of posts that children made themselves, not content written about the data subject.[190] Unlike the right to be forgotten in the EU, the right to be forgotten in the United States is undeveloped.

IV. NONLEGISLATIVE SOLUTIONS TO THE DILEMMA OF PERPETUAL MEMORY

In this part of the Article, we discuss alternative paradigms to operationalize the right to be forgotten.

A. Formation of New Norms Initiated by User Communities

Informal social sanctions, not legal remedies, enforce social norms.[191] If Internet users can agree on the right to be forgotten as a social norm, legal actions over the right to delete may be minimized.

B. Market-Based Approaches

One way to jump start norms is to reshape consumer expectations by pressuring companies that process personally identifiable data to respect a right of erasure. One difficulty with this approach is that companies such as social media sites depend upon the commoditization of personal data. These companies' economic incentive is to

186. *See, e.g.*, N.C. Gen. Stat. Ann. § 90-96 (disqualifying petitioners for expungement who were over 21 years of age at the time of the offense).

187. *Id.* at 238.

188. S.B. 568, 2013 Leg., Reg. Sess. (Cal. 2013).

189. *See id.*

190. *Id.* § 22581(a)(1); Julia McClure, *The Right To Be Forgotten in a Digital Age*, NAT'L SECURITY L. BRIEF (Nov. 14, 2013), http://www.nationalsecuritylawbrief.com/the-right-to-be-forgotten-in-a-digital-age/.

191. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 84 (2007).

gather and spread information, not to restrict it or censor it. Nevertheless, if social norms develop, public demand for control over personal information can influence even the most powerful social media services to adjust their policies or to expand their services to include a right to delete.[192] When Facebook's CEO Mark Zuckerberg remarked that "the rise of social networking online means that people no longer have an expectation of privacy,"[193] he tacitly assumed Facebook is following social norms in making user data more public and accessible as opposed to private and personal.

However, this assumption about the portability of personally identifiable data may soon be outdated. Throughout Europe, there is strong support for a right to be forgotten. Seven out of ten Europeans "are concerned about the potential use that companies may make of the information disclosed."[194] A European Commission study concluded that seventy-five percent of Europeans favor a right to be forgotten.[195] A majority of EU respondents in every member state favor the right to delete personal information with the highest support in Malta (83%) and the Czech Republic, Cyprus and Sweden (all 82%), and the thinnest support in the Netherlands (64%), Bulgaria (66%) and Italy (68%).[196] Several years ago, Facebook unilaterally modified its terms of service by giving users a right to delete content that they post on Facebook.[197] In order for the erasure right to evolve further, however, Facebook users throughout the world will need to demand stronger protections for their private data.[198] Changes in social norms will slowly turn into voluntary agreements and collaboration that will give private subjects an extralegal way to delete postings or pictures. As new norms develop towards a right of erasure among the companies that process personal identifiable data, the issue of being searchable and found in a Google search will solve itself. Since Google Search automatically and constantly crawls the web so that information that no longer exists on a source website will not be found in a search for the data subject's name, the result will be an efficient de-

192. Conley, *supra* note 13, at 58.

193. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), http://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

194. Press Release, Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote, *supra* note 111.

195. Directorate-Gen. Justice, Info. Soc'y & Media & Joint Research Ctr., Eur. Comm'n, *Attitudes on Data Protection and Electronic Identity in the European Union*, 2, Special Eurobarometer 359 (June 2011), *available at* http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

196. *Id.* at 158.

197. Brian Stelter, *Facebook's Users Ask Who Owns Information*, N.Y. TIMES, Feb. 17, 2009, at B3, *available at* http://www.nytimes.com/2009/02/17/technology/internet/17facebook.html.

198. *See* FREDRIK ALVERÉN, SÅLD PÅ NÄTET — PRISET DU BETALAR FÖR GRATIS 213–14 (2012).

linking of personal identifiable data from Google and other search engines.[199]

C. Expiration Dates for Personally Identifiable Data

Another way to reduce takedown notices while solving the problem of the Internet's perpetual memory is to implement expiration dates that would make postings, comments, and other information automatically disappear after a designated period. Under the expiration dates method, the data subject would establish the shelf life for postings or data, and after a designated period, third parties would not be able to save or make copies of the information.

Expiration dates allow the data subject to "act in time" without impairing comprehensive digital memory, which parallels the role that forgetting performs in human decision-making.[200] However, "expiration dates are not about imposed forgetting."[201] Rather, they are about "awareness and human action, and about asking humans to reflect — if only for a few moments — how long the information they want to store may remain valuable and useful."[202] Expiration dates on postings are unlikely to become the new default in the absence of new norms to counter flawless remembering in the digital age.[203] The advantage of expiration dates is that it is the data subject who determines the expiration date for data. The disadvantage is that data may have a continuing vitality after the expiration date due to the public's right to know.

1. Operationalizing Expiration Dates for Personal Data

In order for data subjects to set expiration dates for postings and other data, Google, Facebook, and other companies will need to make it easy to code data with an expiration date. At present, these Internet moguls' business models depend on the perpetual retention, transmission, and sharing of data. If certain data is given a shelf life, data subjects will have peace of mind that postings and pictures depicting youthful indiscretions will not stigmatize them for a lifetime. Expiration dates for postings about a data subject's juvenile offenses would also obviate the need to petition a court to expunge this data and give the data subject a fresh start. Expiration dates would reduce the administrative burden in operationalizing the right to be forgotten. Limiting retention to only up-to-date information would also increase the

199. *See generally* Mei Kobayashi & Koichi Takeda, *Information Retrieval on the Web*, 32 ACM COMPUTING SURVEYS 144 (2000).

200. *See* MAYER-SCHÖNBERGER, *supra* note 4, at 194.

201. *Id.* at 172.

202. *Id.*

203. *Id.* at 169–95.

accuracy of Google's search matches, potentially enhancing the value of data while creating trust among consumers.[204]

The most important variables when discussing expiration dates are time and power. The time challenge of digital remembering is determining how long information should be retained and thus remembered. The data subject must have foresight to accurately set the date for potentially harmful data.[205] Whether this information is relevant in the future may be unforeseeable when the data subject sets the expiration date in the metadata. One possible solution would be to allow the data subject to extend the period of retention after posting. For information related to criminal offenses, the default retention time of the data could be set to the length of time the crime remains on the data subject's criminal record. For information related to a private data subject, the default retention time should be longer where the public interest prevails, for example, where a person signs a petition urging the U.S. Senate to approve a candidate for U.S. Attorney General or provides testimony in response to a Federal Drug Administration request for comment about the efficacy of an over-the-counter drug product or medical device. In both of these cases, the public's right to know would outweigh the private subject's right to expunge or delink the information.

Another undecided issue is who should have the power to decide time limits on data. Under the EU model of privacy, the power to decide should be with the surveyed rather than surveyors.[206] The goal of expiration dates for information is to avoid automation, that is, "not to push the problem of digital memory off our consciousness by delegating it to technology, but rather the opposite: to make humans aware of the value and importance of forgetting."[207] It is unclear whether a data subject's "shelf life" estimate can be extended by public authorities when the posting triggers the public's right to know.

2. Technical Enforcement of a Shelf Life for Data

Expiration dates would be relatively easy to implement, since just as a digital picture may already have metadata such as the date and time it was taken, expiration dates may be seen as just an additional piece of metadata that stores the data's shelf life or life expectancy.[208] Viktor Mayer-Schönberger proposes four ways in which expiration

---

204. *See id.* at 194.

205. One of the main issues with expiration dates for data is the impossibility of foreseeing what should disappear and what will be of public value. This problem increases if a person ultimately becomes a public figure or official, and their public status thereby makes the data relevant and no longer subject to takedown.

206. *Cf.* MAYER-SCHÖNBERGER, *supra* note 4, at 191–92.

207. *Id.* at 185.

208. *Id.* at 173.

dates are a modest response to the demise of forgetting: (1) technically, expiration dates utilize ideas, infrastructures, and mechanisms that already exist or that would require small modifications; (2) legally, there is no need to rely on any new rights or institutions since expiration dates are similar to forgetting in the analogue world; (3) expiration dates are modest in the way they regulate human behavior, which also includes software and law; (4) politically, expiration dates seem to be more acceptable than a regulatory approach, as they are not extremely controversial.[209] By allowing the data subject to determine the shelf life of data, many takedown requests would be obviated.[210]

D. Contextualization

Contextualization gives data subjects the fundamental right to correct information that is inaccurate, false, incomplete, out-of-date, or otherwise inappropriate. Contextualization is "an instrument through which individuals correct and re-project their images to society."[211] Under contextualization, the data subject would provide details updating or explaining an out-of-context or out-of-date posting.[212] Rather than erasing or removing information, contextualization enables users to add more information.[213] The website Rate My Professors employs contextualization by giving professors a right to respond to negative student evaluations.[214]

Public officials and public figures would have the financial and human resources to use contextualization as part of their program of reputation management. If information places a public figure in a false light, the data subject may respond and explain the context. One danger is that public figure data subjects would be able to suppress negative opinions by posting overly positive information and explanations.[215] This contextualization method would most likely be used in response to third parties who have written something about the

209. *Id.* at 189–90.

210. Despite this, it will of course be difficult to remove copies of data that have been downloaded and saved on a desktop, flash drive, or external storage device. The ability to track all such information is likely impossible. Facebook message from David Larochelle, Lead Eng'r, Berkman Ctr. for Internet & Soc'y, Harvard Univ., to author (Apr. 9, 2014) (on file with author). However, the issue of circumventing expiration dates through saving copies on external devices could possibly be solved by making it impossible to post and save the original data if it has no expiration date attached. *See infra* Part IV.C.

211. Norberto Nuno Gomes de Andrade, *Oblivion: The Right To Be Different . . . from Oneself. Re-proposing the Right To Be Forgotten*, *in* MONOGRAPH VII INTERNATIONAL CONFERENCE ON INTERNET, LAW, AND POLITICS, NET NEUTRALITY AND OTHER CHALLENGES FOR THE FUTURE OF THE INTERNET 122, 131 (2012).

212. ZITTRAIN, *supra* note 120, at 229–30.

213. *Id.*

214. *See The Best of "Professors Strike Back,"* RATE MY PROFESSORS, http://blog.ratemyprofessors.com/the-best-of-professors-strike-back (last visited July 10, 2014).

215. *See* ALVERÉN, *supra* note 198, at 194.

data subject. Its impact in reality depends, however, on the data subject's willingness and ability to constantly monitor and act on the existing content about himself or herself online.[216]

Contextualization could most successfully be applied to searches on a search engine. In 2007, Google experimented in this area by introducing a feature that allowed individuals who were mentioned in articles indexed by Google News to add a comment that would appear next to the article.[217] The comment could be an explanation of the information contained in the article, an apology, or an argument to why readers should disregard the content.[218] However, Google later abandoned this feature, a decision that has been criticized in the wake of the decision in *Google Spain v. AEPD* since such a contextualization function could have given data subjects more control over their personal information "without giving [data subjects] the power to censor."[219]

E. Cognitive Adjustment

When discussing the future of forgetting in the digital age, it is important to consider that people, their behavior, and their opinions may evolve.[220] The solution is not to fight the propagation of memory, but to adapt to it. The idea is that no structural invention can combat changes in thinking: "People, particularly younger people, are going to come up with coping mechanisms. That's going to be the shift, not any intervention by a governmental or technological body."[221] The idea of cognitive adjustment is simple since it does not require any changes in society through new laws or technical architectures. The changes will solely take place in our minds. The big question that remains to be answered is how much time such change will take.

---

216. Companies have used the business model of helping people protect their online reputation and control their personal information on the Internet. Among them is Reputation.com, a company that helps users discover what is said about them online, how many people have searched for their name, and whether the results of the search are positive or negative. Reputation.com can also help one push negative content to the bottom of search results and push good content to the top. REPUTATION.COM, http://www.reputation.com/reputationdefender (last visited Feb. 25, 2015).

217. Dan Meredith & Andy Golding, *Perspective About the News from People in the News*, GOOGLE NEWS BLOG (Aug. 7, 2007, 10:32 PM), http://googlenewsblog.blogspot.se/2007/08/perspectives-about-news-from-people-in.html.

218. Jonathan Zittrain, *Don't Force Google To "Forget,"* N.Y. TIMES, May 14, 2014, at A29, *available at* http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html.

219. *Id.*

220. MAYER-SCHÖNBERGER, *supra* note 4, at 154.

221. Jessica Winter, *The Advantages of Amnesia*, BOS. GLOBE (Sept. 23, 2007), http://www.boston.com/news/globe/ideas/articles/2007/09/23/the_advantages_of_amnesia/?page=full.

V. A PROPOSAL TO RECONCEPTUALIZE THE RIGHT TO BE FORGOTTEN TO ACCOMMODATE EXPRESSION

We propose that the European Union narrow its right to be forgotten in order to walk the tightrope between the Scylla of inadequately protecting expression and the Charybdis of diminishing an individual's right to reputation. In this part of the Article, we propose a way to accommodate the right to be forgotten to an increasingly globalized online world.

A. Background

1. The Need to Harmonize the Right To Be Forgotten

Data packets containing personally identifiable information do not report to customs when they cross national borders on the virtual highway; routers do not pause to consider whether privacy norms are being breached. The right to be forgotten will be the law in Europe by 2017.[222] If the United States does not adopt some version of the right to be forgotten, it will need to renegotiate the U.S.-EU Safe Harbor Agreement. The Safe Harbor Agreement between the United States and Europe enables the exporting of personal data from the Eurozone,[223] but Vice-President of the European Commission and EU Justice Commissioner Viviane Reding has contended that the agreement in its current form may not actually be safe at all, since U.S. privacy standards are too low: "[W]e kicked the tyres and saw that repairs are needed. For the Safe Harbour to be fully roadworthy the U.S. will have to service it . . . . [The] Safe Harbour has to be strengthened or it will be suspended."[224] It is therefore imperative for the United States to harmonize its law so that the European Commission classifies U.S.-based privacy policies as reasonably secure. A suspension or revocation of the agreement would have a devastating impact on Facebook and other social networking sites that are currently a part of the agreement.[225] The advantage of our proposal over non-legislative alternatives such as the expiration date or market-based approach[226] is that it will harmonize the law of the United States and Europe, while

222. Press Release, Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote, *supra* note 111; Foster, *supra* note 21.

223. *U.S.-EU Safe Harbor Overview*, *supra* note 74.

224. Viviane Reding also stated, "And finally a message to our American friends . . . Applying different standards to nationals and non-nationals makes no sense in view of the open nature of the internet." Reding, Speech at the Centre for European Policy Studies, *supra* note 112; *see also* Eur. Comm'n, Data Protection Day, *supra* note 115 (arguing for updating the EU's Data Protection Directive to account for changes in information technologies).

225. *See U.S.-EU Safe Harbor List*, EXPORT.GOV, https://safeharbor.export.gov/list.aspx (last visited July 25, 2014).

226. *See supra* Part IV.

also reconciling erasure rights with free expression.[227] It is also exportable to the United States where courts have fifty years of experience balancing the First Amendment against state defamation rights.[228]

2. The Three Degrees of Deletion

The goal of a right to be forgotten under the GDPR is to give all data subjects a right to control their history on the Internet. To enable a better understanding of what type of data might be included in a right to be forgotten and identify the scope of such an erasure right, this part of the Article breaks down the concept.

Peter Fleischer, Google's Global Privacy Counsel, describes three common scenarios for a right to be forgotten on the Internet:

> 1) If I post something online, should I have the right to delete it again? I think most of us agree with this, as the simplest, least controversial case. If I post a photo to my album, I should then later be able to delete it, if I have second thoughts about it. Virtually all online services already offer this, so it's unproblematic, and this is the crux of what the French government sponsored in its recent Charter on the Droit a l'Oubli. But there's a big disconnect between a user's deleting content from his/her own site, and whether the user can in fact delete it from the Internet (which is what users usually want to do), more below.
>
> 2) If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it? This is the classic real-world case. For example, let's say I regret having posted that picture of myself covered in mud, and after posting it on my own site, and then later deleting it, I discover someone else has copied it and re-posted it on their own site. Clearly, I should be able to ask the person who re-posted my picture to take it down. But if they refuse, or just don't respond, or are not find-able, what can do [sic] I do? I can pursue judicial procedures, but those are expensive and time-consuming. I can

227. *GDPR*, *supra* note 15, art. 17(3), at 52.

228. *See* Anna S. Persky, *50 Years After* New York Times v. Sullivan*, Do Courts Still Value Journalists' Watchdog Role?*, ABA J. (Mar. 1, 2014), http://www.abajournal.com/magazine/article/50_years_after_new_york_times_v._sullivan_do_courts_still_value_journalists.

> go directly to the platform hosting the content, and if the content violates their terms of service or obviously violates the law, I can ask them to take it down. But practically, if I ask a platform to delete a picture of me from someone else's album, without the album owner's consent, and only based on my request, it puts the platform in the very difficult or impossible position of arbitrating between my privacy claim and the album owner's freedom of expression. It's also debatable whether, as a public policy matter, we want to have platforms arbitrate such dilemmas. Perhaps this is best resolved by allowing each platform to define its own policies on this, since they could legitimately go either way.
>
> 3) If someone else posts something about me, should I have a right to delete it? Virtually all of us would agree that this raises difficult issues of conflict between freedom of expression and privacy. Traditional law has mechanisms, like defamation and libel law, to allow a person to seek redress against someone who publishes untrue information about him. Granted, the mechanisms are time-consuming and expensive, but the legal standards are long-standing and fairly clear. But a privacy claim is not based on untruth. I cannot see how such a right could be introduced without severely infringing on freedom of speech. This is why I think privacy is the new black in censorship fashion.[229]

Under Fleischer's model, the first degree of deletion is when a data subject publishes a posting, picture, or comment. In other words, the posting, picture, or comment originates with the data subject.[230] Second-degree deletion, according to Fleischer's model, is where the data originates with the data subject but is reposted. In other words, the data subject posts a picture or comment, and someone else copies and reposts it on his or her own site.[231] The rationale for second-degree deletion is that the data subject retains a privacy interest, even if he or she voluntarily posted that information in a public forum. This

---

229. Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY . . . ? (Mar. 9, 2011), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

230. "*Example*: The subject deletes an embarrassing photo she posted in her own Twitter feed." Larsen, *supra* note 162, at 12.

231. "*Example*: One of the subject's Twitter followers copied the photo and reposted it on Facebook, and now the subject wants it deleted." *Id.*

right pits the data subject's right of control over information about himself or herself against another poster's freedom of expression.[232] Fleischer's third degree of deletion is when third parties comment on, write about, or take pictures of the data subject and post the content online.[233] While second-degree deletion also clashes with the freedom of expression, the third-degree of deletion poses the greatest threat to a democratic society, because it involves deleting a third party's comments, postings, or pictures.

Although Fleischer's three degrees of deletion refer to deletion of the content itself and our reform proposal refers to deletion of links, his framework will be critically important to our proposal to narrow Article 17 of the proposed GDPR. Table 1 below summarizes the three degrees of deletion.

Table 1: Three Degrees of Deletion

Degree of Deletion	Description	Examples
First degree of deletion	Data subject's own postings and pictures online.	Data subject posts embarrassing pictures of himself on Facebook and seeks to erase them.
Second degree of deletion	Data subject posts content that a third party copies and reposts on the third party's own site.	Data subject posts on Twitter, and third party retweets it on her own site. Data subject seeks removal of retweet.
Third degree of deletion	Third party posts data not created by the data subject but that is about the data subject.	Third party posts picture of or data about data subject on Facebook. Data subject requests removal of posting.

a. First Degree of Deletion: Erasing Data Originating from the Data Subject

The first degree of deletion gives data subjects a right to take down their own tweets, postings, and pictures. This degree is the least objectionable and poses the lowest risk to freedom of expression. To a large extent, data subjects already have the right to erase their own postings on Facebook and other social networking sites.[234] For exam-

232. Fleischer, *Foggy Thinking About the Right to Oblivion*, *supra* note 229.

233. "*Example*: A newspaper posts an article about the subject's misconduct, and she wants it deleted." Larsen, *supra* note 162, at 13.

234. *See, e.g.*, *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last updated Jan. 30, 2015).

ple, Twitter gives users instructions to delete first-degree, but not second- or third-degree tweets:

> Did you Tweet something and then change your mind? Don't worry! It's easy to delete one of your Tweets. Please note that you can only delete Tweets that you have made, you cannot delete other users' Tweets from your timeline.[235]

Similarly, Facebook grants users the right to untag unflattering pictures, comments, and postings.[236] Facebook's privacy settings also give users the ability to control some of the information they share with the other billion users.[237] Deletion on such a basic level has become increasingly popular with the photo messaging application Snapchat, where deletion is the default setting.[238] With self-destructing messages as its core concept, the sender of a Snapchat picture can determine the length of time the recipient has to view it, after which the message disappears from the recipient's device and is deleted from Snapchat's servers.[239] No other social media website currently establishes deletion so that content automatically disappears after a designated period.[240]

---

235. *Deleting a Tweet*, TWITTER, https://support.twitter.com/articles/18906-deleting-a-tweet# (last visited June 28, 2014).

236. *What If I Don't Like Something I Am Tagged In?*, FACEBOOK, https://www.facebook.com/help/196434507090362 (last updated May 2014).

237. *Data Use Policy — Facebook*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Jan. 30, 2015). However, despite the risk of reputational damage, "[a]lmost 13 million users said they had never set, or didn't know about, Facebook's privacy tools. And 28 percent shared all, or almost all, of their wall posts with an audience wider than just their friends." *Facebook & Your Privacy*, CONSUMER REP. MAG. (June 2012), http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm (reporting the results of a survey conducted by the Consumer Reports National Research Center). Unless the user takes affirmative action to control access, his or her profile will be viewable to the public by default.

Further, Facebook may actually retain the information a user deletes. A study by Austrian law student Max Schrem reported that Schrem's request to Facebook to provide him with all of his personal data yielded 1222 pages of posts, comments, and pictures, some of which he thought he had deleted, but that Facebook had actually saved. Mona Tömböl & Philippe Schennach, EU v. Facebook*: Fighting for the Right To Be Forgotten*, VIENNA REV. (Feb. 5, 2013), http://www.viennareview.net/news/special-report/eu-vs-facebook-fighting-for-the-right-to-be-forgotten.

238. *See Privacy Policy*, SNAPCHAT, https://www.snapchat.com/privacy (last updated Nov. 17, 2014).

239. *Id.*

240. Although no website yet has deletion as a default setting, they may look at Snapchat with regard to their easy-to-control social media technology. Snapchat's new invention, for which the company filed for patent protection in May 2014, can "make it very obvious to users which content goes on their public profile and which content goes on a private profile only they can see." Alyson Shontell, *Is This Snapchat's Secret Plan To Best Facebook?*, BUS. INSIDER (July 26, 2014, 7:31 AM), http://www.businessinsider.com.au/snapchat-social-profiles-patent-2014-7.

U.S. politicians have exercised the first degree of deletion in recent years. For example, Mississippi Senator Thad Cochran and Massachusetts Representative Stephen Lynch deleted tweets that supported the release of Bowe Bergdahl from the Taliban as the backlash against his rescue grew, according to an organization that tracks deleted tweets.[241] In another case involving public officials, tweets about the U.S. Senator of New Hampshire Senator Jeanne Shaheen's attendance at a fundraiser to discuss the Affordable Care Act's effect on New Hampshire's healthcare system were deleted.[242] Senator John McCain also deleted the following tweet: "Dear Vlad, Surprise! Surprise! You won. The people of #Russia are crying too" after Vladimir Putin won the presidential election.[243]

Cases where public officials such as Senators Shaheen or McCain delete or delink their own posts arguably rewrites history especially when the posts relate to controversial public issues or general public policies. A key issue is to determine when a public official's posts have a nexus to the public's right to know or a public issue. Senator Shaheen's posts on healthcare policy are a classic example of posts that have a strong connection to a public interest. However, suppose that Senator Shaheen posted a comment about how much she enjoyed her Labrador retriever's antics or her child's high school graduation. While she is a public official, comments about her dog or her children will not normally implicate the public's right to know, and under our proposal a public official would be able to remove links to such postings. A public official would only have a right to delete postings with no connection to their public role.

b. Second Degree of Deletion: Erasing Reposted Data that Originated from the Data Subject

The second degree of deletion is when the data subject posts something and someone else copies and reposts it on his or her own site. The second degree of deletion is illustrated by a data subject's postings on Facebook or Twitter that are reposted or retweeted by another social network user. Second-degree erasure would protect the data subjects from friends, family, or third parties who have reposted or tagged the data subject in potentially incriminating content:

---

241. Margaret Talev et al., *Obama Says "No Apologies" for Exchange To Free Bergdahl*, Bloomberg (June 5, 2014), http://www.bloomberg.com/news/articles/2014-06-05/obama-says-he-has-no-apologies-for-exchange-to-free-bergdahl.

242. Targeted News Service, *New Hampshire GOP: Shaheen Lobbyist Fundraiser Tweets Vanish After Criticism*, INS. NEWS NET (June 25, 2014), http://insurancenewsnet.com/oarticle/2014/06/25/new-hampshire-gop-shaheen-lobbyist-fundraiser-tweets-vanish-after-criticism-a-522165.html.

243. Samantha Bare, *Tweet, Delete, Repeat: Politicians Turn a Microphone into a Megaphone*, CRONKITE NEWS (June 1, 2012), http://cronkitenewsonline.com/2012/06/tweet-delete-repeat-politicians-turn-a-microscope-into-a-megaphone.

> Be especially careful about who tags you in their posts, including photos. I recently saw that a Friend had been tagged in their Friend's photos. Naturally, I was curious, so I clicked to see what the photos were about. Boy, was I surprised! The people in the photos were clearly very drunk, some were smoking a bit of the wacky weed and I saw exposed body parts that I really hadn't wanted to see!
>
> The Friend in question is extremely professional. He's someone I've known for several years. More importantly, *he* wasn't in any of the photos. His buddy had tagged him because he thought it was funny. Unfortunately, my Friend was up for a promotion and he was Friends with his boss...who didn't think the photos were funny at all.
>
> The easiest way around this is to set your own Privacy settings so that you have to approve it when someone tags you. Unfortunately, my Friend didn't know this and it cost him a promotion.[244]

Copyright law's distinction between expression and ideas is a useful analogy in reconceptualizing second-degree deletion. In copyright law, protection is given to expressive content, but not to ideas.[245] A picture or posting that the data subject created and publishes online is protectable under copyright law, and a third-party reposter infringes on the copyright by reposting without the owner's permission or license.[246] However, it is not copyright infringement to merely link to a data subject's picture or posting.[247] The Canadian Supreme Court in *Crookes v. Newton*[248] held that a mere hyperlink could not be considered a publication.[249] Thus, a mere link to a data subject's posting or picture is only a reference to content, not a distinct publication.

---

244. Deb Krier, *Social Media: Guilt by Association*, SOCIALIGHT, http://debkrier.com/social-media-guilt-by-association/ (last visited Mar. 5, 2015).

245. *See* Conley, *supra* note 13, at 55.

246. Under the Copyright Act, copying means that a defendant has infringed one or more of the copyright owner's six exclusive rights under 17 U.S.C. § 106 (2012). These exclusive rights include the rights to reproduce, distribute, publicly display, publicly perform, publicly perform by digital audio transmission, and create derivative works of the copyrighted work. *Id.*

247. Bernstein v. J.C. Penney, Inc., No. 98-2958 R EX, 1998 WL 906644, at *1 (C.D. Cal. 1998).

248. [2011] 3 S.C.R. 269 (Can.).

249. *Id.* ¶ 44; Gregory B. Bordan, *Developments in Internet Law: Defamation and Hyperlinks*, NORTON ROSE FULBRIGHT (Nov. 2011), http://www.nortonrosefulbright.com/knowledge/publications/58001/developments-in-internet-law-defamation-and-hyperlinks.

Under second-order deletion, data subjects can request that the reposter remove from the social media site pictures the data subject himself took. In the United States, section 230 of the Communications Decency Act ("CDA")[250] does not impose a duty on websites to remove defamatory postings upon notice by the data subject.[251] By contrast, under Article 17 of the GDPR, EU citizens retain the right to control information about themselves, even if they previously released that information to the public.[252] This overly expansive privacy right gives a data subject the right to delete an embarrassing photo or comment that he or she posted — even if another data subject has copied it.[253] In this scenario, the data subject is effectively asking the platform to choose between the privacy right of the data subject to have a picture deleted and the freedom of expression of the person who has posted it to his or her wall or online photo album.[254] Vint Cerf, one of the Internet's founding fathers, identifies a common denominator between the analog and the virtual world in the following vivid example:

> The analogue [equivalent of this digital idea] is terrifying; if somebody said "I want everyone to forget about this book that I published because it's embarrassing", how would you implement that? You would have to break in to people's homes and take the book off the bookshelves. There's some legal issues with that and it seems to me that it shouldn't be any easier in the online world.[255]

In implementing the second degree of deletion, it would be impossible to completely erase all digital footprints of a posting or picture that originated with the data subject but was subsequently tagged or reposted by third parties.[256] For example, a reposted picture may be copied onto a flash drive and viewed on a personal computer without

---

250. Communications Decency Act (CDA), 47 U.S.C. § 230 (2012). The CDA sought to preserve the "vibrant and competitive free market" of ideas on the Internet. 47 U.S.C. § 230(b)(2).

251. Zeran v. Am. Online, 129 F.3d 327, 333 (4th Cir. 1997) ("If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement — from any party, concerning any message.").

252. *GDPR*, *supra* note 15, art. 17, at 51.

253. *Id.* art. 17(2), at 51.

254. *See* Fleischer, *Foggy Thinking About the Right to Oblivion*, *supra* note 229.

255. Matt Warman, *Vint Cerf Attacks European Internet Policy*, TELEGRAPH (Mar. 29, 2012), http://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html.

256. Facebook message from David Larochelle to author, *supra* note 210. *See generally* LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 5 (2012) (stating that "what happens in Facebook doesn't stay in Facebook").

access to the Internet. The most realistic way of achieving the second degree of deletion would be to place the burden of identifying an objectionable link on the data subject.

c. Third Degree of Deletion: Erasing Other People's Data About the Data Subject

The third right to be forgotten scenario is when a third party posts content about the data subject that forms the basis of a takedown request. A dramatic example of a third degree deletion request is the case *Doe v. Franco Productions.*[257] There, the court awarded more than $500 million to college athletes secretly filmed by Internet pornographers.[258] The plaintiff's lawsuit was based upon claims for invasion of privacy, unlawful use of the plaintiffs' images for monetary gain, and mail and wire fraud under civil RICO laws.[259] The pornographers set up hidden cameras in dressing rooms and showers to film hundreds of college athletes in various degrees of nudity at locker rooms, restrooms, and wrestling meets.[260] The secret videotapes claimed to show "hot young dudes" and were posted on adult subscription entertainment websites.[261] The Seventh Circuit held that the Internet service provider was not liable for any tort because of the broad immunity granted to providers by section 230 of the CDA.[262]

Another illustration of a third-degree takedown request concerns LiveLeak's display of a video of Max Mosley, the President of Formula One, with five prostitutes who were described as dressing as Nazis.[263] In the United States, Mosley would be classified as a public figure because of his high profile role in international racing.[264] Thus,

257. No. 99 C 7885, 2000 WL 816779 (N.D. Ill. June 22, 2000).

258. Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 111 (2003) (discussing *Franco* verdict, subsequent procedural history leading to default judgment against primary defendants, and section 230 immunity for website hosts).

259. *Id.*

260. 2000 WL 816779, at *1.

261. Rustad & Koenig, *supra* note 258, at 111.

262. *See* Doe v. GTE Corp., 347 F.3d 655, 655, 659–60 (7th Cir. 2003).

263. Miranda Miller, *Google Won't Erase Links to Max Mosley Hooker Orgy Stories, So He Sues*, SEARCH ENGINE WATCH (Dec. 15, 2011), http://searchenginewatch.com/sew/news/2133193/google-wont-erase-links-max-mosley-hooker-orgy-stories-sues#; Chris Crum, *Former Formula One Head Wants Google To Remove Results Showcasing Infamous Orgy*, WEBPRONEWS (Sept. 6, 2013), http://www.webpronews.com/former-formula-one-head-wants-google-to-remove-results-showcasing-infamous-orgy-2013-09.

264. *See* Curtis Publ'g Co. v. Butts, 388 U.S. 130 (1967) (pronouncing the public figure standard in the United States); *Max Mosley: "Endless List" of Public Figures with Interesting Sex Lives*, BBC (Feb. 3, 2010), http://news.bbc.co.uk/today/hi/today/newsid_8495000/8495232.stm; *see also* Steven Glover, *A Sordid Orgy and Why Max Mosley Can't Be Allowed To Erase History*, DAILY MAIL (Sept. 11, 2013), http://www.dailymail.co.uk/debate/article-2418040/A-sordid-orgy-Max-Mosley-allowed-erase-history.html ("Mr Justice Eady ruled that if it had been a Nazi orgy he might have found in favour of the newspaper, since Mr Mosley was a public figure of sorts whose suit-

Mosley's demand to Google to take down the video would pit the right of takedown against the public's right to know.[265] Under our scaled back right to be forgotten reform, a public figure such as Mosley as well as public officials would have no right to take down links to third-party postings that have a nexus to the public interest. In contrast, the college athletes victimized by secret filming in *Franco Productions* would have that right. The public has a right to know a public figure's alleged Nazi predispositions, but has no right to view the naked bodies of college athletes who have been filmed without consent. Further, public officials and public figures such as Mosley generally have the financial resources and political acumen to correct the record if the information was false or misleading. However, plaintiffs like the college athletes likely will have more difficulty restoring their reputations when a website has widely distributed their nude images.

The websites sued in Franco Productions are examples of "merchant of misery" websites, which use a business model predicated upon degradation of the data subject shown.[266] The website Mugshots posts pictures and booking information obtained from public law enforcement websites and provides a toll-free number by which a depicted person can get their picture taken down for a fee.[267] JailBase provides a searchable database of criminal records by first and last name.[268] JailBase states,

> Arrest and booking records simply state who, when and why (if available) someone was arrested or booked. It does not imply guilt. An arrested or booked individual is innocent until proven guilty in a

---

ability for his high-profile job would have been seriously called into question by such antics.").

265. *See, e.g.*, Aoife White & Angeline Benoit, *"Google It" Becomes "Hide It" After Right To Be Forgotten*, BLOOMBERG (July 9, 2014), http://www.bloomberg.com/news/2014-07-09/-google-it-becomes-hide-it-after-right-to-be-forgotten.html (quoting Mosley who said, "You have to draw the line somewhere and if Google won't do it, which they should, then the courts will have to act.").

266. *See Misery Merchants: How Should Online Publication of Explicit Images Without Their Subjects' Consent Be Punished?*, ECONOMIST (July 5, 2014), http://www.economist.com/news/international/21606307-how-should-online-publication-explicit-images-without-their-subjects-consent-be; Sanna Kulevska, *Who Owns the Right to Your Face? Websites Cash in on Internet Mugshots*, CHILLING EFFECTS (July 8, 2013), http://www.chillingeffects.org/weather.cgi?WeatherID=814 ("[E]ven if the mugshot sites are within their First Amendment right as a redistribution of public records, this general rule can be nullified by the fact that they are requiring money to have it taken down: 'Anybody who wants to exploit your image for commercial gain has to pay you, just like you're licensing copyright.'").

267. MUGSHOTS, http://mugshots.com/US-Counties/New-Jersey/Morris-County-NJ (last visited Feb. 19, 2014).

268. *What Is JailBase?*, JAILBASE, http://www.jailbase.com/en/about (last visited Feb. 19, 2014).

> court of law. What happens in a court of law (for example, when charges are dropped), is outside the scope of Jailbase.com . . . .[269]

However, this disclosure does not remove the disgrace to a person depicted on a mug shot who was acquitted or whose charges were dismissed.

Another example of misery merchants are the 3000 or more websites that feature revenge pornography, explicit images of intimacies that can damage "future relationships and careers."[270] One revenge porn website, UGotPosted, published explicit images of victims while another site, ChangeMyReputation, charged $300 or more to have the images removed.[271] A former NFL football player is being sued by his ex-wife for allegedly posting pornographic images of her on several websites without her knowledge or consent.[272] In another example, an ex-boyfriend distributed nude pictures of a female high school student, and she later committed suicide as a result of harassment by her classmates.[273] In a recent court case, Facebook was sued for not removing nude pictures of a plaintiff from its website fast enough.[274] Internet wrongdoers have also used new morphing technologies to superimpose a victim's face onto pornographic images.[275] As a result of re-

---

269. *Id.*

270. *Misery Merchants: How Should Online Publication of Explicit Images Without Their Subjects' Consent Be Punished?*, *supra* note 266.

271. *Id.* Before UGotPosted was shut down, it housed tens of thousands of nude images of women and their personal information, such as name, address and age. ChangeMyReputation charged more than $300 to remove images from UGotPosted. The business models of both websites were based on annoying data subjects and extracting settlements from them to remove materials posted without their consent by third parties such as ex-husbands or ex-lovers. *See* Jordan Larson, *Alleged Revenge Porn Webmaster Faces Trial in California*, VICE NEWS (June 17, 2014), https://news.vice.com/article/alleged-revenge-porn-webmaster-faces-trial-in-california.

272. *Suit: Former NFL Player Published Explicit Images of Ex-Wife Without Permission*, 89 WLS (Mar. 5, 2014), http://www.wlsam.com/common/page.php?pt=Suit:+Former+NFL+player+published+explicit+images+of+exwife+without+permission&id=87883.

273. Kim Zetter, *Parents of Dead Teen Sue School over Sexting Images*, WIRED (Dec. 8, 2009), http://www.wired.com/2009/12/sexting-suit.

274. Josh Wolford, *Facebook Sued over "Revenge Porn" Page*, WEBPRONEWS (July 30, 2014). In this case, a woman from Texas sued Facebook for $123 million for delaying the removal of nude pictures depicting her in sexual acts. The pictures, which were posted by her ex-boyfriend, gestalts a different type of revenge porn, since her actual face was paired with photoshopped nude bodies of other people.

275. *Flight Attendant Wins Sexual Harassment Suit*, 9 TEX. EMPLOYMENT L. LETTER 6 (1998), *available at* 9 No. 9 Tex. Employment L. Letter 6 (Westlaw) (discussing *Butler v. Crabbs* and *Continental Express*). The flight attendant alleged that "the pilot took her picture with a digital camera and then used computer equipment to alter it. The result was an image of the flight attendant superimposed on a bikini-clad model from a Sports Illustrated swimsuit edition" and "photographs of her face superimposed on photographs of nude women." *Id. But cf.* Blakey v. Cont'l Airlines, Inc., 730 A.2d 854, 856 (N.J. 1999) (dismissing female pilots' defamation, invasion of privacy, and sexual harassment claims involving postings by male pilots on airline's intranet bulletin board on personal jurisdiction grounds), *rev'd and remanded on other grounds*, 751 A.2d 538, 543 (N.J. 2000).

venge pornography, "women were branded thots (a slang word for slut) and their nude pictures commented upon and retweeted" on Facebook, Instagram, and other social media platforms.[276] These websites perpetuate digital stigmas that will negatively affect reputation forever, unless expunged.

Under U.S. law, if a website refuses to take down or untag allegedly defamatory or tortious content, there is no legal ground for compelling a website to do so because section 230 of the CDA imposes no duty on websites as service providers to take down information even if the information constitutes an ongoing tort.[277] Nor does the Digital Millennium Copyright Act ("DMCA") give the subject of a posting a right to untag material reposted by a third party unless the data subject holds the copyright to the images or other content.[278] Even if content about a plaintiff is posted in a manner that constitutes an ongoing tort, he or she has no cause of action against the website, as long as the website cannot be classified a content creator. In *Directory Assistants, Inc. v. SuperMedia, LLC*,[279] an advertising consulting agency filed defamation and tortious interference with contract claims against SuperMedia and three of its employees, because the company distributed hyperlinks to allegedly defamatory material on Ripoff Report and another site.[280] The plaintiffs also alleged that SuperMedia sent these hyperlinks to third-party customers and potential customers.[281] The court dismissed all claims against SuperMedia on the basis of its immunity under section 230 of the CDA.[282] The CDA shields interactive computer services from claims that seek to treat them as the publisher or speaker of information originating from a third party user of the service.[283]

The United States District Court for the Northern District of Georgia ruled similarly in *Chaney v. Fayette County Public School*

---

276. Hannah Jane Parkinson, *Twitter Trend Based on the Purge Films Exposes Horror of Revenge Porn*, GUARDIAN (July 21, 2014), http://www.theguardian.com/technology/2014/jul/21/twitter-trend-purge-film-anarchy-revenge-porn-laws.

277. 47 U.S.C. § 230 (2012).

278. *See* Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512 (2012).

279. 884 F. Supp. 2d 446 (E.D. Va. 2012).

280. *Id.* at 448.

281. *Id.*

282. *Id.* at 453.

283. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). The court found that the CDA "precludes courts from entertaining claims that would place a computer service provider in a publisher's role," and therefore bars "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content." *Id.* The CDA defines interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2) (2012).

District.[284] In that case, a school district showed an embarrassing picture of a high school student accompanied by her full name at a seminar designed to illustrate the permanency of social media postings.[285] The student filed suit, charging that the school falsely depicted her as a "sexually-promiscuous abuser of alcohol who should be more careful about her Internet postings."[286] The court ruled that the student, even though she was a minor, had no right to privacy in the photograph because she had intentionally shared the photograph online with groups of friends.[287] However, if the student had password protected the image, the court might have reached a different outcome.[288] The prior cases demonstrate that courts are generally unwilling to order takedowns even when postings constitute an ongoing tort such as the invasion of privacy. A plaintiff's only recourse is to request a website voluntarily take down an objectionable posting, which the website might only do if the posting clearly violates its policy on acceptable content.

Our reform proposal aims to drive out of business misery merchants who remove salacious or humiliating content if the subject pays. Under our version of the right to be forgotten, private persons would have a right to delink objectionable information posted by a third party that serves no purpose other than to embarrass or extort payment. This third degree of the right to be forgotten is most likely in conflict with the freedom of expression[289] but mainly limiting the right to private parties minimizes the chilling impact on speech.

3. *Google Spain v. AEPD*'s Collision with Freedom of Expression

The recent *Google Spain v. AEPD* case, where a Spanish citizen asked Google to remove search results linking to articles about his past debts, is another example of a third-degree deletion demand. Such a demand is particularly controversial because it gives a right of erasure for truthful comments, postings, or pictures about the data subject that may be of interest to the public.[290] For example, potential busi-

284. 977 F. Supp. 2d 1308 (N.D. Ga. 2013).

285. *Id.* at 1312.

286. *Id.*

287. *Id.* at 1316.

288. *Cf.* R.S. *ex rel*. S.S. v. Minnewaska Area School Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) (holding "that one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence," and thus, "based on established Fourth Amendment precedent, that R.S. had a reasonable expectation of privacy to her private Facebook information and messages").

289. *See* Fleischer, *Foggy Thinking About the Right to Oblivion*, *supra* note 229.

290. One prominent privacy commentator on the *Google Spain v. AEPD* case interprets the decision as allowing search engines to be reticent towards taking down content about public figures. "The ruling seems to give search engines more leeway to dismiss take-down requests for links to webpages about public figures, in which the information is deemed to be of public interest. But search engines may err on the side of caution and remove more

ness partners and investors are entitled to know that a person with whom they are considering doing business was declared insolvent. If the third degree of deletion is construed too broadly in protecting a data subject's private sphere from third-party postings, there will be inevitable censorship or rewriting of the past.[291]

B. Extending N.Y. Times v. Sullivan *to the Right To Be Forgotten*

Our right to be forgotten proposal imports the distinction between private persons, public figures, and public officials recognized by *New York Times v. Sullivan*[292] and its progeny to determine who has standing to initiate takedown demands.[293] Just as in U.S. defamation law, the distinction between private persons and public officials or figures balances the data subject's right of privacy with the fundamental right of freedom of expression. U.S. courts have balanced these rights for the past fifty years, ruling that torts must give way to free expression.[294] Just as U.S. courts have made defamation subject to the First Amendment, we extend this well-established constitutional framework to scale back the right to be forgotten.

Under our reform proposal, private individuals, public officials, and public figures will have a right to be forgotten for the first two degrees of deletion: links to data originating with the data subject and data originating with the data subject that is reposted by third parties.[295] Private persons would have a right to be forgotten for third-degree deletions of links to websites that serve no purpose other than to cause emotional distress or extort payment for removal. Public officials and figures would have no right to erase links to data about them originating with third parties, unless the data was published with actual malice and has no nexus to the public interest. All requests will also be subject to a general exemption for the public's right to know. The proposed reform provides data controllers, including search engines, principled grounds for refusing takedown or de-indexing requests for public officials and public figures. It recognizes that the right to be forgotten is more limited for public officials and public figures than

---

links than necessary to avoid liability." Alexei Oreskovic, *"Right To Be Forgotten": Google Hit with Takedown Requests After European Court Ruling*, RAW STORY (May 14, 2014), http://www.rawstory.com/rs/2014/05/14/right-to-be-forgotten-google-hit-with-takedown-requests-after-european-court-ruling.

291. *See* David Mitchell, *supra* note 148 ("No one has the right to be forgotten, any more than they have the right to be remembered. Our only right in this regard should be not to be lied about . . . I wouldn't think less of someone because his house was repossessed 16 years ago. But I would if he turned out to be a liar.").

292. 376 U.S. 254 (1964).

293. *See* Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365, 382 (2013).

294. *See* Persky, *supra* note 228.

295. Only human persons, not corporations or other entities, would have a right of takedown.

for private data subjects. Indeed, the European Commission-appointed Article 29 Working Party has recently acknowledged that the right to be forgotten is more restricted for "politicians, senior public officials, business-people and members of the (regulated) professions."[296]

1. *New York Times v. Sullivan* and Its Progeny

a. The First Amendment and Private Persons

The standard of fault in a defamation per se case is negligence if the plaintiff is a private figure, in contrast to actual malice if the plaintiff is a public official or public figure.[297] In *Doe v. Friendfinder Network, Inc.*,[298] a New Hampshire Jane Doe plaintiff filed a defamation suit against Friendfinder Network, the operator of an adult networking site, because an anonymous third party had created a false profile of her using the screen name "petra03755" and depicted her as a "swinger."[299] The court granted Friendfinder Network's motion to dismiss the plaintiff's claims for invasion of privacy and defamation, under the federal immunity provided by CDA Section 230.[300] It ruled that the defendant was an interactive service provider and not a content creator because someone else had created the allegedly defamatory profile page,[301] and the website was not transformed into a content provider merely because it made slight modifications to the plaintiff's profile.[302]

---

296. In November of 2014, the Article 29 Working Party endorsed the following criteria for search engines to consider when processing delisting requests: "Does the data subject play a role in public life? Is the data subject a public figure?" Article 29 Data Prot. Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "*Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*" C-131/12, 13*, WP 225 (Nov. 26, 2014) [hereinafter Article 29 Data Prot. Working Party, *Guidelines on the Implementation of* Google Spain v. AEPD], *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. A report published by the Advisory Council to Google on the Right To Be Forgotten, a council that Google convened for advice on how to implement the right to be forgotten, also addressed the issue of evaluating the data subject's role in public life. THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN, THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7–8 (2015), http://www.scribd.com/doc/254900585/Report-of-the-Advisory-Committee-to-Google-on-the-Right-to-Be-Forgotten. The Article 29 Working Party's *Guidelines on the Implementation of* Google Spain v. AEPD and the report by the Advisory Council to Google are not discussed in more detail because they were released three and six months, respectively, after we submitted this Article to the *Harvard Journal of Law and Technology*.

297. Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 755–57 (1985) (Powell, J.) (plurality opinion).

298. 540 F. Supp. 2d 288 (D.N.H. 2008).

299. *Id.* at 291–92.

300. *Id.* at 298, 306.

301. *Id.* at 294–95.

302. *Id.* at 297–98.

b. The First Amendment and Public Officials

In U.S. defamation law, it is well-established that a person who is a public official bears a heavy burden of proof because his "position [is] one which would invite public scrutiny and discussion of the person holding it."[303]After *Sullivan*, a public official was required to prove, by clear and convincing evidence, that a false and defamatory statement was made against him or her with actual malice — in other words, that the defendant either knew the statement was false or acted with reckless disregard as to the truth or falsity of the statement.[304] The *Sullivan* court did not define the term "public official" and did not specify whether lower level employees of the government were included.[305] The Court's decision to make it almost impossible for public officials to pursue defamation action was predicated on a "profound national commitment" to "uninhibited, robust, and wide-open" debate that "may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."[306]

Europe has a dignity-based approach to privacy, which historically has prevailed over liberty and expression.[307] In Europe, defamation claims of public officials are rarely successful due to the wording in Article 10 of the ECHR, which underscores that the public has a right to impart information and ideas on political issues and matters of general interest.[308] Because of the need to balance such a right with the "protection of reputation of others," the freedom of political debate as necessary to a democratic society prevails throughout the European Court of Human Rights.[309] Therefore, "[t]he limits of acceptable criticism are accordingly wider with regard to a politician acting in his public capacity than in relation to a private individual."[310] In Europe, defamation

303. Rosenblatt v. Baer, 383 U.S. 75, 86–87 n.13 (1966).

304. New York Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964); *see also* Curtis Publ'g Co. v. Butts, 388 U.S. 130, 145 (1967) (extending *New York Times* to public figures and stating that the burden of proof is clear and convincing evidence).

305. 376 U.S. at 283 n.23.

306. *Id.* at 270.

307. *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160–61 (2004) (comparing Europe's dignity-based approach to privacy to America's liberty-based approach).

308. ECHR, *supra* note 22, 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. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.").

309. *See* Maud De Boer-Buquicchio, Deputy Sec'y Gen., Council of Eur., Opening Address at the Regional Conference on Defamation and Freedom of Expression (Oct. 17, 2002), *available at* http://www.coe.int/t/dghl/standardsetting/media/doc/H-ATCM(2003)001_en.pdf.

310. Oberschlick v. Austria (No. 1), 19 E.H.R.R. 389, 422 (1991).

laws differ between the member states.[311] However, truth and "justification" of the publication of an allegedly defamatory statement is a defense in most European countries, just as in the United States.[312]

c. The First Amendment and General Public Figures

In the United States, the reputation of public figures, like those of public officials, are afforded less protection than those of private persons. Under the general public figure test, there is a high bar for celebrities and other qualifying persons to receive defamation damages.[313] In *Curtis Publ'g Co. v. Butts*,[314] the Court extended the *New York Times* decision from public officials to public figures.[315] The Court in *Gertz v. Robert Welch, Inc*.[316] further distinguished between general purpose public figures and limited purpose public figures.[317] General public figures are plaintiffs who are famous or celebrities who have earned widespread fame or notoriety.[318] Famous basketball players such as Michael Jordan or Lebron James easily qualify as public figures as do entertainers such as Madonna, Paul McCartney, or Rihanna. "The defendant who can show that his plaintiff is a public figure can hold that plaintiff to a higher standard of proof, forcing him to prove that the defendant was reckless, rather than negligent."[319] To be liable for defamation of a public figure, a distributor of allegedly defamatory material must act with actual malice.[320]

---

311. In some member states, the national law defines defamation as a criminal offense, while in other member states it is a civil wrong. *See* Sanna Kulevska & Maria S. Ciaburri, Berkman Ctr. for Internet & Soc'y, Harvard Univ., Spreadsheet: Defamation Laws Worldwide (Aug. 2013), https://docs.google.com/spreadsheet/ccc?key=0AmNE4-fBw--mdFdvbUZjeTN5WjFWQ2E2RlpzekRYRVE&usp=drive_web#gid=0. The purpose of this research was to create an overview of defamation laws in different legal systems in order for U.S.-based companies to better understand the national laws with which to comply when receiving takedown requests from individuals living outside the United States. Knowledge in the specific national defamation law related to the complainant in question is vital for U.S. companies when removing defamatory content from the national country code top-level domain ("ccTLD").

312. *See* Council of Eur., *supra* note 311; New York Times Co. v. Sullivan, 376 U.S. 254, 279 (1964).

313. *See* Thomas D. Brooks, *Catching Jellyfish in the Internet: The Public-Figure Doctrine and Defamation on Computer Bulletin Boards*, 21 RUTGERS COMPUTER & TECH. L.J. 461, 475 (1995).

314. 388 U.S. 130 (1967).

315. *Id.* at 155.

316. 418 U.S. 323 (1974).

317. *Id.* at 352.

318. Tavoulareas v. Piro, 817 F.2d 762, 772 (D.C. Cir. 1987), *cert. denied*, 484 U.S. 870 (1987) (stating that a person becomes a general purpose public figure only if his name is a "household word").

319. Brooks, *supra* note 313, at 461.

320. *Curtis Publ'g Co*., 388 U.S. at 155; Russell Hickey, *Refashioning Actual Malice: Protecting Free Speech in the Right of Publicity Era*, 41 TORT TRIAL & INS. PRAC. L.J. 1101, 1101 (2006).

The United States is the bellwether jurisdiction in making the tort of defamation subject to free speech.[321] In the United States, liberty trumps "personality, honor and human dignity," which are higher values in other countries.[322] Whereas Europe has led the world in conceptualizing privacy as dignity, the United States has conceptualized privacy as liberty.[323] The freedom of expression in defamation cases is less developed in the Eurozone than in the United States. In the United Kingdom, for example, public figures often seek so-called "super injunctions" to block media organizations from writing about them, in stories discussing their sex scandals for example, and they have the means to do so.[324]

> The injunctions are so protective of their subjects that only a few cases have been made public: John Terry, the captain of the English soccer team, who was reported to have had an affair with the ex-girlfriend of a teammate; Fred Goodwin, the former chairman of the $40 billion banking group Royal Bank of Scotland, who faced criticism for his lavish payouts; and Trafigura, a multinational commodities company accused of dumping toxic waste in Africa.[325]

Other UK super injunctions have been imposed to protect prominent public men, which likely reflects the court's protection of "our ruling class[,] that a public figure's sex life should always be private, however aberrant it may be."[326] Similarly in Australia, public figures

---

321. Rick Pildes, *How the Doctrine of "Responsible Journalism" Has Changed Journalism and Defamation Law in Canada and the UK*, BALKINIZATION (Mar. 19, 2014, 12:16 PM), http://balkin.blogspot.com/2014/03/how-doctrine-of-responsible-journalism.html ("Ever since *New York Times v. Sullivan* (1964) . . . the United States has struck the balance between public debate and legitimate reputational interests of public figures more heavily in favor of public debate than in any other country.").

322. Webchat with Donald Kommers, Professor, Univ. of Notre Dame (Mar. 1, 2006).

323. Whitman, *supra* note 307, at 1160–61 ("Continental European and American sensibilities about privacy grow out of much larger and much older differences over basic legal values . . . between privacy as an aspect of dignity and privacy as an aspect of liberty.").

324. Stephen Glover, *Silenced in Courts; Stephen Glover on Why Judges Cover Up Sleaze of the Rich and Famous*, DAILY MIRROR, Apr. 5, 2011, at 8; Yessir, *David and Victoria Beckham in Global Hunt for Hooker Irma Nici*, A BIG MESSAGE (Sept. 25, 2010), http://www.abigmessage.com/david-and-victoria-beckham-in-global-hunt-for-hooker-irma-nici.html (discussing the use of super injunctions by English footballers David Beckham and Wayne Rooney).

325. Ravi Somaiya, *British Law Used To Shush Scandal Has Become One*, N.Y. TIMES, Apr. 27, 2011, at A4, *available at* http://www.nytimes.com/2011/04/27/world/europe/27britain.html.

326. Stephen Glover, *Why Are Our Judges Covering Up the Sleazy Behaviour of Public Figures?*, DAILY MAIL (Apr. 5, 2011), http://www.dailymail.co.uk/debate/article-1371789/Why-judges-covering-public-figures-sleazy-behaviour-superinjunctions.html; *see also* John Kampfner, *The Worrying Rise of the Rich Man's Weapon of Justice*, INDEPENDENT, Apr. 1,

and public officials are not treated differently than private persons by defamation laws.[327] Our proposal is that the European and U.S. standards for the right to be forgotten explicitly recognize the distinction between private persons, public officials, and public figures.

d. The First Amendment and Limited Public Figures

The U.S. Supreme Court created the limited purpose public figure classification to "define the proper accommodation between the law of defamation and the freedoms of speech and press protected by the First Amendment."[328] Limited public figures are those data subjects who have voluntarily injected themselves into a particular public controversy; they become public figures for that limited range of issues.[329] In contrast, a general purpose public figure has such "pervasive fame or notoriety that he becomes a public figure for all purposes and in all contexts."[330] The U.S. Supreme Court narrowed the meaning of the limited purpose public figure classification in *Time, Inc. v. Firestone*,[331] where it held that Mary Firestone, a famous socialite who had attended a press conference about her divorce, was a private person and not a limited purpose public figure.[332] The Court found that Firestone had done nothing to "thrust herself to the forefront of any particular public controversy in order to influence the resolution of the issues involved in it."[333] In a Minnesota libel case, a court ruled that a community blogger was a limited public figure who committed defamation, after intentionally interfering with a former community leader's employment contract through his blog and the associated comments.[334]

Table 2 summarizes the different categories of plaintiffs and the corresponding standards of proof needed to show defamation.

2011, at 14, *available at* http://www.independent.co.uk/voices/commentators/john-kampfner-the-worrying-rise-of-the-rich-mans-weapon-of-justice-2258869.html (noting that gag orders are being granted in favor of the rich and powerful, thereby chilling legitimate journalism and public inquiry).

327. Denis Muller, *Defamation Law Reform Stalled*, AGE, Oct. 26, 1992, at 13, *available at* 1992 WLNR 5403430.

328. Gertz v. Robert Welch, Inc., 418 U.S. 323, 325 (1974).

329. *See, e.g.*, Gulrajaney v. Petricha, 885 A.2d 496, 505 (N.J. Super. Ct. App. Div. 2005) (finding that a candidate in a runoff election for a condominium association was a limited rather than a general purpose public figure).

330. *Gertz*, 418 U.S. at 351.

331. 424 U.S. 448 (1976).

332. *Id.* at 453–55.

333. *Id.* at 453.

334. Verdict and Settlement Summary, Moore v. Allen, No. 27-CV-09-17778, 2011 WL 3622928 (Minn. Dist. Ct. Mar. 11, 2011).

Table 2: Plaintiff's Status and Standards of Proof for Defamation

Type of Plaintiff	Definition	Standard of Proof for Defamation	Emblematic Examples
Private person	Person not classifiable as either a public official or public figure.	Negligence.[335]	Mary Firestone, a prominent socialite, was a private person for purposes of a libel lawsuit because she did "not thrust herself to the forefront of any particular public controversey" by appearing at a press conference about her divorce.[336]
Public official	"Those among the hierarchy of government employees who have, or appear to the public to have, substantial responsibility for or control over the conduct of governmental affairs" and where that position "has such apparent importance that the public has an independent interest in the qualifications and performance of the person who holds it, beyond the general public interest in the qualifications and performance of all government employees . . . ."[337]	"[C]onvincing clarity" that the statements were made with "actual malice."[338]	A speaker who criticized a public official's fitness for office was not held to be liable for defamation.[339]

335. Brooks, *supra* note 313, at 461.
336. Time, Inc. v. Firestone, 424 U.S. 448, 453, 454–55 n. 3 (1976).
337. Rosenblatt v. Baer, 383 U.S. 75, 85, 87 (1966).
338. New York Times Co. v. Sullivan, 376 U.S. 254, 285–86, 279–80 (1964).
339. Condit v. Dunne, 317 F. Supp. 2d 344 (S.D.N.Y. 2004).

General purpose public figure	Plaintiffs who are celebrities or otherwise famous. "Few people . . . attain the general notoriety that would make them public figures for all purposes."[340]	Same as public official.	"[A] well-known athlete or entertainer[,] . . . archetypes of the general purpose public figure."[341]
Limited purpose public figure	Those who have voluntarily injected themselves into a particular public controversy and "assume[d] special prominence in the resolution of public questions." They become public figures for that limited range of issues.[342]	Same as public official.	Attorney who represented the Pagans motorcycle gang was a limited public figure.[343]

2. Operationalizing the Right To Be Forgotten To Balance Expression

Our reform proposal to balance the EU's right to be forgotten with the fundamental freedom of expression draws heavily upon the U.S. Supreme Court decisions on the law of defamation, beginning with the 1964 case of *New York Times v. Sullivan* that has been the law for a half-century. The EU Commission already makes the right of erasure subject to free expression under Article 17(3) of the GDPR.[344] Under our right to be forgotten proposal, private persons will have a presumed right to be forgotten for the first two degrees of deletion. For the third degree of deletion, private persons will be able to demand delinking to content that serves no purpose other than to embarrass or extort a settlement. Public officials, general public figures, and limited public figures will have a right to be forgotten ex-

340. Waldbaum v. Fairchild Publ'ns, Inc., 627 F.2d 1287, 1290, 1296 (D.C. Cir. 1980) (ruling that the president of the second largest cooperative in the country was only a limited public figure); *see also* Wolston v. Reader's Digest Ass'n, 443 U.S. 157, 165 (1979).

341. Tavoulareas v. Piro, 817 F.2d 762, 772 (D.C. Cir. 1987).

342. Gertz v. Robert Welch, Inc., 418 U.S. 323, 351 (1974).

343. Marcone v. Penthouse Int'l Magazine for Men, 754 F.2d 1072, 1075 (3d Cir. 1985) (ruling that an attorney's voluntary connection with motorcycle gangs was sufficient to make him a public figure).

344. *GDPR*, *supra* note 15, art. 17(3), at 52.

tending to first- and second-degrees of deletion. However, they will generally not have a right to third-degree erasure. Our proposal acknowledges that public officials and public figures forgo some of their privacy interests when entering the world of politics and fame. An individual's right to be forgotten ceases once he or she "step[s] into the public arena."[345] Congressman Anthony Weiner, for example, would have no right to takedown for sending photographs of his penis because he was a public official.[346] The sole exception is the removal of links to content that was published with actual malice and no longer serves any legitimate public purpose, such as purloined sex tapes and similarly embarrassing information.[347]

Further, all categories of takedown requests will be subject to a compelling public interest for disclosure, which will be defined as case law develops.[348] The public interest factor will provide data controllers additional flexibility when distinguishing between private persons, public officials, and public figures. Table 3 below summarizes our reform proposal to narrow the EU's right to be forgotten to balance privacy with expression.

Table 3: Data Subject's Status and Right To Be Forgotten

Type of Data Subject	**First Degree of Deletion**	**Second Degree of Deletion**	**Third Degree of Deletion**
Private Person	Right of removal, unless there is a compelling public	Right of removal, unless there is a compelling public	No right of removal, unless there is proof that

345. *The U.S. Should Adopt the "Right To Be Forgotten" Online*, INTELLIGENCE SQUARED U.S. DEBATES (Mar. 11, 2015), http://intelligencesquaredus.org/debates/upcoming-debates/item/1252-the-u-s-should-adopt-the-right-to-be-forgotten-online (Paul Nemitz, Director for Fundamental Rights and Union Citizenship in the Directorate-General for Justice of the European Commission, discussing the right to be forgotten in Europe).

346. *Misery Merchants: How Should Online Publication of Explicit Images Without Their Subjects' Consent Be Punished?*, *supra* note 270.

347. *See, e.g.*, Bosley v. WildWetT.com, 310 F. Supp. 2d 914, 936 (N.D. Ohio 2004) (enjoining adult entertainment website from commercial use of video showing female news anchor in various stages of undress); Michaels v. Internet Entm't Grp., 5 F. Supp. 2d 823 (C.D. Cal. 1998) (enjoining ClubLove from distributing a private sex tape of musician Brett Michaels and actress Pamela Anderson Lee).

348. In November 2014, the Article 29 Working Party adopted a public interest and public figure criterion for delisting. The Working Group's public interest criterion states, "The CJEU has made an exception for de-listing requests from data subjects that play a role in public life, where there is an interest of the public in having access to information about them. This criterion is broader than the 'public figures' criterion." Article 29 Data Prot. Working Party, *Guidelines on the Implementation of* Google Spain v. AEPD, *supra* note 296, at 13. The Working Party acknowledged the difficulty of defining the sphere of application of the public interest exception, what it constitutes, and which data requests are impacted by this interest. *Id.*

There is still no legislated statute of limitations for how long information of public value shall remain on the web. However, expiration dates for data has been proposed by Professor Viktor Mayer-Schönberger, *see* MAYER-SCHÖNBERGER, *supra* note 4, at 169–95, and was discussed in Part IV.

	interest in the information.[349]	interest in the information.	the posted information no longer serves any purpose other than to cause emotional distress or to extort a settlement[350] or there is no compelling public interest in the information.[351]
Public Official	Right of removal, unless there is a compelling public interest in the information.	Right of removal, unless there is a compelling public interest in the information.	No right of removal, unless the poster acted with actual malice and the information serves no legitimate public purpose.[352]

349. This limited public interest exception only applies to private persons who do not qualify as limited public figures because they have not injected themselves into public issues. *See* Mathis v. Cannon, 573 S.E.2d 376, 381–82 (Ga. 2002) (holding that a frequent poster on a Yahoo message board was classified as a limited public figure because he injected himself into a public debate over the unprofitable operation of a local solid waste recovery facility). Private data subjects could weigh in on a public controversy but not qualify as a limited public figure where, for example, a private person signs a petition to the Food and Drug Administration ("FDA") calling for labeling of genetically engineered foods. There, a private individual would not have a right of removal because the petition urges a federal agency to take a certain action and has a nexus to the public interest. The FDA, for example, publishes citizen petitions for stays of agency action on specific drugs and medical devices. *See* FOOD & DRUG ADMIN., OMB CONTROL NO. 0910-0679, CITIZEN PETITIONS AND PETITIONS FOR STAY OF ACTION SUBJECT TO SECTION 505(Q) OF THE FEDERAL FOOD, DRUG, AND COSMETIC ACT: GUIDANCE FOR INDUSTRY (2014), *available at* http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm079353.pdf; Memorandum from June G. Brown, Inspector Gen., Dep't of Health & Human Services, to Michael A. Friedman, Lead Deputy Comm'r, Food & Drug Admin. (July 17, 1998), *available at* https://oig.hhs.gov/oas/reports/phs/c9750002.pdf ("Any interested person may submit written comments on a petition to the Dockets Management Branch, and these comments become part of the docket file.").

However, search engines may nonetheless grant a request for takedown by a private individual even where the posting relates to a public issue if that posting is stale (for example, two years after the citizen petition) or inaccurate (for example, where a scrivener errs in transmitting the citizen's petition).

350. Examples are mug shot and revenge porn websites. A data subject would also be able to erase credit card numbers, social security numbers, or other personally identifiable information posted without permission by third parties.

351. Third-party data postings about doctors, clergy, community leaders, or police are presumptively in the public interest, even though they may be private figures under libel law.

352. The proposal recognizes a narrow right to be forgotten for public officials and public figures where the posting is purely about the person's private life and has no nexus to the public's right to know. The Article 29 Working Party also endorses a right to be forgotten for public figures for purely private information. The Working Party states:

> There may be information about public figures that is genuinely private and that should not normally appear in search results, for example information about their health or family members. But as a rule of

General Purpose Public Figure	Same as public official.	Same as public official.	Same as public official.
Limited Purpose Public Figure	Same as public official.	Same as public official.	Same as public official.

3. Balancing Third-Degree Deletion Requests and the Freedom of Expression

In right to be forgotten cases, a fair balance must be struck between the right of reputational reset for data subjects and the right of free expression, which varies significantly between countries. With hundreds of countries connected to the Internet, it is unclear whose community standards apply. The same information posted on the Internet may be protected in North America, for example, while considered offensive by non-Western countries that value personal honor over expression.[353] An Islamic fundamentalist female might be held in contempt for appearing on a website that shows her unveiled face. A Hindu might be humiliated if she was unwittingly featured in a hamburger chain's online advertisement. The concern is that there will be a race to the bottom towards adopting the norms of the most restrictive legal system.

Under the rubric of privacy, Forget.me reported that the most common data requests sought removal of the data subject's home address (N=66, 22%), followed by negative opinions about the data subject (N=55, 18%).[354] The next largest category was requests for redundant information to be deleted (N=49, 16%), followed by data on origin, nationality, or ethnic identity (N=25, 8%).[355] Other privacy-related requests concerned the data subject's academic performance, philosophical beliefs, religious beliefs, income, political views, sexual orientation, health status, and union membership.[356]

Under our proposed reform, private persons would likely be unsuccessful in requesting delinking of information posted by third parties unless they could show the website was extorting a settlement from them in exchange for removing information, for example merchant of misery websites which include revenge porn and mug shot

---

> thumb, if applicants are public figures, and the information in question does not constitute genuinely private information, there will be a stronger argument against de-listing search results relating to them.

Article 29 Data Prot. Working Party, *Guidelines on the Implementation of* Google Spain v. AEPD, *supra* note 296, at 14.

353. *See* Kulevska & Ciaburri, *supra* note 311.

354. Natasha Lomas, *Forget.me Puts out Early Data on What Europeans Want To Vanish from Google*, TECHCRUNCH (June 30, 2014), http://techcrunch.com/2014/06/30/forget-me-early-data/.

355. *Id.*

356. *Id.*

websites.[357] Under our reform proposal, none of these examples of third-degree postings implicate the public's right to know, and takedown requests to remove links to them should be granted. This part of our proposal aims to wholly eliminate merchant of misery websites. Table 4 provides a typology of takedown requests that a search engine should presumptively grant.

Table 4: Examples of Third-Degree Deletion Demands Granted Under the Proposal[358]

Information To Be Delinked	Policy Justification
Non-consensual publication of explicit images such as private sex tapes.[359]	Images serve no purpose other than to humiliate.
Mug shots of the data subject.	Reputational fresh start for the data subject where he or she has had charges dropped, been acquitted, or finished serving the sentence.[360]
Jerk.com's practice of harvesting profiles from Facebook and encouraging Jerk.com's users to make negative comments.[361]	Jerk.com serves no purpose and profits from humiliating social media users. Some profiles contained personally identifiable information such as work and home addresses, and a "Jerk" rating could have a viral effect when viewed by strangers, acquaintances, friends, family members, employers, and future employers.

In general, requests by public officials and public figures for the delinking of posts originating from third parties would not succeed

357. *See supra* Part V.A.2.c.

358. Table 4's categories apply whether the data subject is a private person, public official, or public figure. However, if the data subject is a public official or public figure, this factor is weighed against a takedown request.

359. For example, a Texas jury awarded $500,000 in damages to a woman whose ex-boyfriend posted salacious images of her taken from a Skype call. Andrew, *Woman Awarded $0.5m in Revenge Porn Lawsuit*, LEGAL RADAR (Mar. 7, 2014), http://www.legalradar.com/2014/03/woman-awarded-05m-in-revenge-porn-lawsuit.html; *see also* Matthew Goldstein, *Law Firm Founds Project to Fight "Revenge Porn,"* N.Y. TIMES (Jan. 29, 2015), http://dealbook.nytimes.com/2015/01/29/law-firm-founds-project-to-fight-revenge-porn/?_r=3.

360. *See generally* Horace Boothroyd III, *Racism: 78% of Black Youth Arrested in Oakland Never Charged*, DAILY KOS (Aug. 29, 2013, 8:06 AM), http://www.dailykos.com/story/2013/08/29/1234743/-Racism-78-of-Black-youth-arrested-in-Oakland-never-charged#; Benjamin Weiser, *5 Exonerated in Central Park Jogger Case Agree To Settle Suit for $40 Million*, N.Y. TIMES (June 19, 2014), http://www.nytimes.com/2014/06/20/nyregion/5-exonerated-in-central-park-jogger-case-are-to-settle-suit-for-40-million.html?_r=0.

361. In April 2014, the Federal Trade Commission charged Jerk, LLC with a pattern of deceptive representation. Complaint at 5–6, Jerk, LLC, d/b/a Jerk.com, F.T.C. No. 9361 (Apr. 7, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140407jerkpart3cmpt.pdf. Jerk.com profiles often appeared in search engine results when a person searched for an individual's name. *Id.*

under our proposal. For example, the request demanding takedown of links to the German actor's Wikipedia entry[362] would be rejected under our proposal because of the public's right to know. Wolfgang Werlè and Manfred Lauber had brutally murdered a German actor, and after serving time in prison one of the men requested that Wikimedia remove references to his conviction, a public record, from the Wikipedia entry of the actor.[363] The lawyers representing the data subjects contended that removal was required under German law to protect the name and likeness of private persons from unwanted publicity.[364] Our reform to the erasure right would deny the takedown request because the data subjects became limited public figures by murdering a famous actor and thereby thrust themselves into the public spotlight.[365] Table 5 presents a sample of other takedown requests from public officials and figures that would be denied under our reform.

Table 5: Examples of Third-Degree Deletion Demands from Public Officials and Public Figures Denied Under the Proposal

Data Subject	**Information To Be Delinked**	**Result Under Our Reform**
Former Merrill Lynch Chief Executive	Blog entry stating that the data subject was forced to leave the company after bank suffered huge losses.[366]	Denied: Third-degree deletion request involving general public figure.

362. *See supra* Part II.E.2.

363. Bundesgerichtshof [BGH] [Federal Court of Justice] July 21, 1994, Entscheidungen des Bundesgerichtshofes in Strafsachen [BGHSt] 40, 211 (Ger.), *available at* http://www.hrr-strafrecht.de/hrr/1/94/1-83-94.php; Meg L. Ambrose & Jef Ausloos, *The Right To Be Forgotten Across the Pond*, 3 J. INFO. POL'Y 1, 3 (2013).

364. *Id.*; *see also* Jennifer Granick, *Convicted Murdered to Wikipedia: Shhh!*, ELECTRONIC FRONTIER FOUND. (Nov. 10, 2009), https://www.eff.org/deeplinks/2009/11/murderer-wikipedia-shhh.

365. The prohibition on third-degree deletions by public officials and public figures would also apply to solicitors seeking offices in bar associations. In the aftermath of *Google Spain v. AEPD*, the search engine gave no reasons for delinking articles such as an article about a solicitor who was seeking a seat on the Law Society's ruling body and facing a fraud trial. James Ball, *EU's Right To Be Forgotten: Guardian Articles Have Been Hidden by Google*, GUARDIAN (July 2, 2014), http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google.

366. Robert Peston, *Merrill's Mess*, BBC (Oct. 29, 2007), http://www.bbc.co.uk/blogs/legacy/thereporters/robertpeston/2007/10/merrills_mess.html (the blog entry that Merrill Lynch executive requested be removed); Keith Perry, *BBC's Robert Peston: "Why Has Google Cast Me into Oblivion?,"* TELEGRAPH (July 3, 2014), http://www.telegraph.co.uk/technology/google/10942429/BBCs-Robert-Peston-Why-has-Google-cast-me-into-oblivion.html (discussing Google's delinking of BBC article).

Former President of the Law Society	Eleven-year-old news story alleging that Robert Sayer created "a phantom identity in order to have his former deputy expelled from the profession."[367]	Denied: Third-degree deletion request involving public figure (either general or limited).
George Osborne's brother	Story about George Osborne's brother's conversion to Islam and the brother's suspension from the practice of medicine after being found guilty of serious misconduct when he falsified a prescription for drugs for an escort.[368]	Denied: Third-degree deletion request involving a relative of a public figure (either general or limited).
Kelly Osbourne, TV star and daughter of rock music couple Ozzy and Sharon Osbourne	News story about Kelly Osbourne leaving the hospital after a seizure.[369]	Denied: Third-degree deletion request involving general public figure.
President of the Law Society	Newspaper article that Robert Sayer described his opponent as a "dog turd" and "a complete pillock."[370]	Denied: Third-degree deletion request involving public figure (either general or limited).
Oxford University archeologist	"An archaeology specialist tried to steal £200 worth of Christmas presents by hiding them in his child's pushchair."[371]	Denied: Third-degree deletion request involving limited public figure.

367. Sally Pook, *Law Society Chief "Faked Claims Against Asian Deputy*,*"* TELEGRAPH (Aug. 8, 2003), http://www.telegraph.co.uk/news/uknews/1438268/Law-Society-chief-faked-claims-against-Asian-deputy.html.

368. *See* Matthew Holehouse & Rhiannon Williams, *Google's Right To Be Forgotten Hides Islamic Marriage of Osborne's Brother*, TELEGRAPH (July 4, 2014), http://www.telegraph.co.uk/technology/google/10947009/Googles-right-to-be-forgotten-hides-Islamic-marriage-of-Osbornes-brother.html.

369. *Kelly Osbourne Leaves Hospital After Seizure*, SKY NEWS (Mar. 13, 2013), https://uk.news.yahoo.com/kelly-osbourne-leaves-hospital-seizure-233542091.html.

370. Robert Verkaik, *"Foul-Mouthed" New Head of Law Society*, INDEPENDENT (July 13, 1999), http://www.independent.co.uk/news/foulmouthed-new-head-of-law-society-1106108.html ("'Every year,' said Mr Sayer, 'Mears comes up like a piece of dog turd on your shoe.'").

371. *Archeology Specialist "Tried To Steal from Shop*,*"* OXFORD MAIL (May 5, 2006), http://www.oxfordmail.co.uk/news/yourtown/oxford/750076.Archaeology_specialist__tried_to_steal_from_shop_/.

Retired Scottish Premier League referee Dougie McDonald	*The Guardian* articles about his resignation after he was found to have lied about his reasons for granting a penalty in a Celtic v. Dundee United match.[372]	Denied: Third-degree deletion request involving public figure (either general or limited).[373]

As Table 5 reveals, many third-degree link takedown requests by public officials and public figures would be denied by data controllers. Although one concern with our reform is that it scales back the right to be forgotten too much, that issue could be resolved by seeking the nonlegislative solutions discussed above to supplement, but not supplant, the right to be forgotten.[374]

4. Data Link Delisting Forms

When evaluating a request to delink data, data controllers must balance the data subject's right to be forgotten against any public interest in the information.[375] Google considers a number of factors in deciding whether to grant a takedown request: "Does it come from a credible news source? How recent is the information? Does it involve political speech? Does the information come from a government?"[376] Microsoft's Bing requires data subjects to complete a four-part form.[377] Our proposal would require data subjects to not only authenticate their identity and authority to take down content,[378] but also

372. Ewan Murray, *Referee at Centre of Celtic Penalty Incident Escapes with a Warning*, GUARDIAN (Oct. 29, 2010), http://www.theguardian.com/football/2010/oct/29/dougie-mcdonald-sfa-warning-penalty-celtic; *see also* Ball, *supra* note 365.

373. Google restored links to these articles about the disgraced referee after *The Guardian* complained of censorship. Alexei Oreskovic & Aurindom Mukherjee, *Google Reverses Decision To Delete British Newspaper Links*, REUTERS (July 4, 2014), http://www.reuters.com/article/2014/07/04/us-google-searches-idUSKBN0F82L920140704.

374. *See supra* Part IV.

375. Google's current data link delisting procedure examines whether data is outdated and "balance[s] the privacy rights of the individual with the public's right to know and distribute information." David Meyer, *Google Starts Taking European Personal Data Link Removal Requests After Privacy Ruling*, GIGAOM (May 30, 2014), https://gigaom.com/2014/05/30/google-starts-taking-european-personal-data-link-removal-requests-after-privacy-ruling.

376. Lance Whitney, *Google Grappling with 70,000 "Right To Be Forgotten" Results*, CNET (July 11, 2014), http://www.cnet.com/news/google-grappling-with-70000-right-to-be-forgotten-requests.

377. *Request To Block Bing Search Results in Europe*, *supra* note 106.

378. Under the proposal, the person seeking delisting must be either the data subject or a person acting with authority from the data subject, such as an attorney. Google's webform requires data subjects making delisting requests to prove their identity. "Those requesting information removal are required to verify their identity by submitting a copy of an identity document such as a driver's licence, national ID card or other photo ID." Natasha Lomas, *Google Offers Webform to Comply with Europe's "Right To Be Forgotten" Ruling*,

provide information that will determine whether they are private persons, public officials, or public figures. Search engines will need a template to make decisions on how a data subject should be classified. Easy cases will be public officials and public figures such as entertainers and famous athletes. The data form must ask probing questions to determine whether a given data subject is a limited public figure. As search engines gain experience with processing requests, the tests for private persons, public figures, and public officials will evolve. The data request form will also require the data subject to disclose whether the data that is the subject of the request originated with them, was reposted, or originated with a third party.

a. Vetting Takedown Requests

Google, which has the largest share of the search engine market, received 12,000 takedown requests within the first twenty-four hours after it posted its online takedown form in Europe.[379] Of the requests that Google received and reviewed for de-indexing, Google granted 41.3 percent.[380] Microsoft, too, has begun to receive takedown requests but its share of the European search engine market is much smaller.[381] Forget.me, an online service for locating and submitting data requests to Google and Bing, released an analysis of 1106 requests by private individuals to de-index outdated or irrelevant personal information from Google.[382] If takedown requests further evolve, the Internet will soon resemble Swiss cheese, with hundreds of millions of holes representing deleted links to stories.

Search engines need a template to determine whether to deny or grant de-indexing requests. As search engines gain experience processing requests, they will hone the template. Data protection authorities in the European Union are only just beginning to develop guidelines or legal bases for processing de-indexing requests.[383] Our

---

TECHCRUNCH (May 30, 2014), http://techcrunch.com/2014/05/30/right-to-be-forgotten-webform.

379. Danny Sullivan, *Google's Right To Be Forgotten Form Gets 12,000 Submissions on First Day*, MARKETING LAND (May 30, 2014), http://marketingland.com/google-right-to-be-forgotten-first-day-85641.

380. *European Privacy Requests for Search Removals*, GOOGLE, http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en (last updated May 1, 2015).

381. Mark Scott, *Microsoft Taking Steps To Comply with the Right To Be Forgotten*, N.Y. TIMES (July 9, 2014), http://bits.blogs.nytimes.com/2014/07/09/microsoft-to-wade-into-complying-with-the-right-to-be-forgotten (noting that Bing accounts for less than three percent of the search engine market in Europe as compared to eleven percent in North America). Ask.com has less than a one percent share of Europe's search engine market and receives only a "small number of requests." *Id.*

382. Lomas, *Forget.me Puts out Early Data on What Europeans Want To Vanish from Google*, *supra* note 354.

383. *See* Press Release, Article 29 Data Prot. Working Party, European DPAs Meet with Search Engines on the "Right To Be Forgotten" (July 25, 2014), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/

proposal for a template is already partially implemented by Google and Bing. In contrast to Google's automated web form for removal requests, Bing's web form requires data subjects demanding erasure to determine whether he or she is a private person or public official/public figure.[384] Google has already adopted a de facto policy of rejecting takedown requests from Members of Parliament who demand the removal of embarrassing material from search results.[385] Google is also expected to deny many celebrities' takedown demands on the grounds of the public's right to know.[386] Google CEO Larry Page contends that "'everyday people' [have] a more legitimate right to seek link suppression" than public figures where there is a "public interest to know."[387] Bing's takedown form similarly requires data subjects to state their privacy interest in removing links to data and why the request outweighs the public's right to know.[388] Authenticating data requests will minimize bogus takedown demands that have the potential of misleading the public or chilling speech. Erasure rights should not violate the "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[389]

b. Burden of Locating URLs on the Data Subject

Our proposal requires data subjects to name specific URLs in their takedown requests, which parallels the present procedure for

---

20140725_wp29_press_release_right_to_be_forgotten.pdf. In July 2014, the Article 29 Data Protection Working Party met to discuss and begin developing guidelines for data protection authorities when deciding whether or not to de-index search results. *See id.*

384. *Request To Block Bing Search Results in Europe*, *supra* note 106; *see also Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited Apr. 4, 2015).

385. Mark Duell, *Google "Will Turn Down Requests from MPs and Celebrities Who Demand Embarrassing Material Is Removed from Search Results,"* DAILY MAIL (June 29, 2014), http://www.dailymail.co.uk/news/article-2673913/Google-turn-requests-MPs-celebrities-demand-embarrassing-material-removed-search-results.html.

386. Rhiannon Williams, *Larry Page: Many Celebrity "Right To Be Forgotten" Requests Likely To Be Denied*, TELEGRAPH (May 30, 2014), http://www.telegraph.co.uk/technology/google/10864332/Larry-Page-many-celebrity-right-to-be-forgotten-requests-likely-to-be-denied.html.

387. *Id.*

388. *Request To Block Bing Search Results in Europe*, *supra* note 106. Part 2 of Bing's takedown form, for example, requires data subjects to disclose their role in society. Data subjects must answer two preliminary questions about whether they are a public figure or official or expect to be one. If the answer is "yes" to either, the data subject must present supporting facts detailing the circumstance. *Id.* In addition, the data subject must specifically describe the content that relates to him or her and give a reason why he or she is requesting the data be blocked by indicating whether the information is "inaccurate or false, incomplete or inadequate, out-of-date or no longer relevant, [or] excessive or otherwise inappropriate." *Id.*

389. New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

DMCA takedown requests.[390] This requirement reduces the burden on data controllers.[391]

VI. CONCLUSION: REMEMBERING AND FORGETTING IN THE DIGITAL AGE

"Time heals all wounds," "memory fades," "forgive and forget." We have all heard these aphorisms, but the Internet has relegated them to the ashbin of history. Because of digitalization, cheap storage, easy retrieval, and globalization, we have moved from an analog system, where indiscretions could be erased or overcome by time, to a digital age where "our pasts are becoming etched like a tattoo into our digital skins,"[392] The perpetual nature of Internet content has led the European Union to adopt a far-reaching right to be forgotten that extends to postings that originate with third parties as well as data by the data subject and data that is reposted. This extended right in its present form cannot coexist with freedom of expression, and this Article has thus proposed a reform to reconcile the two rights. This is a propitious moment to reform the right to be forgotten because the European Commission has not yet articulated how to strike the proper balance between privacy and the freedom of expression.

Due to the global nature of the Internet, European user data is constantly crossing international borders to reach U.S. websites and search engines. In the United States, data subjects have no right to be forgotten, and data can be eternally retrievable by Google, Bing, or other search engines. No state laws, federal statutes, or common law give data subjects control over their data. The difference in approaches to privacy rights can be attributed to America's unilateral protection of the freedoms of expression and the press under the First Amendment and Europe's recognition of the countervailing right to private life in Article 8 of the ECHR. It is a question of liberty versus dignity and privacy.[393]

In this Article, we have proposed harmonizing U.S. and European law by narrowing the right to be forgotten to apply mostly to private persons and limiting the right for public officials and public figures. We have also proposed reducing the right to be forgotten to infor-

---

390. 17 U.S.C. § 512(c)(3)(A) (2012).

391. Microsoft already requires the data subject to identify the specific URL to be blocked in the results of searches of the data subject's name in Bing. *Request To Block Bing Search Results in Europe*, *supra* note 106.

392. J.D. Lasica, *The Net Never Forgets*, SALON (Nov. 25, 1998), http://www.salon.com/1998/11/25/feature_253; *see also* Jessica Winter, *The Advantages of Amnesia*, BOS. GLOBE (Sept. 23, 2007), http://www.boston.com/news/globe/ideas/articles/2007/09/23/the_advantages_of_amnesia/.

393. *See generally* REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY (1999).

mation posted by the data subject or reposted by others, not data originating with third parties. Our shrinking of the right to be forgotten extends this reconceptualized right to be forgotten for the United States as well as Europe.

In narrowing the EU right to be forgotten, we have imported a U.S. constitutional framework refined over fifty years of defamation cases. By mostly limiting this right to private persons, rather than public officials or public figures, the proposal can achieve transatlantic harmonization of data privacy laws. As presently formulated, the right to be forgotten threatens to overwhelm Google in an ocean of takedown requests. For the Internet to work globally, we need international collaboration, rather than an ultimatum from the European Union to the United States. Our proposal gives private subjects a legislative right to be forgotten that respects free expression and thereby enables transatlantic data flow.