PROPOSAL FOR AN INTERNATIONAL TAXONOMY ON THE VARIOUS FORMS OF THE "RIGHT TO BE FORGOTTEN": A STUDY ON THE CONVERGENCE OF NORMS

W. GREGORY VOSS* AND CÉLINE CASTETS-RENARD**

The term "right to be forgotten" is used today to represent a multitude of rights, and this fact causes difficulties in interpretation, analysis, and comprehension of such rights. These rights have become of utmost importance due to the increased risks to the privacy of individuals on the Internet, where social media, blogs, fora, and other outlets have entered into common use as part of human expression. Search engines, as Internet intermediaries, have been enrolled to assist in the attempt to regulate the Internet, and the rights falling under the moniker of the "right to be forgotten," without truly knowing the extent of the related rights. In part to alleviate such problems, and focusing on digital technology and media, this paper proposes a taxonomy to identify various rights from different countries, which today are often regrouped under the banner "right to be forgotten," and to do so in an understandable and coherent way. As an integral part of this exercise, this study aims to measure the extent to which there is a convergence of legal rules internationally in order to regulate private life on the Internet and to elucidate the impact that the important Google Spain "right to be forgotten" ruling of the Court of Justice of the European Union has had on law in other jurisdictions on this matter.

This paper will first introduce the definition and context of the "right to be forgotten." Second, it will trace some of the sources of the rights discussed around the world to survey various forms of the "right to be

* Professor of Business Law, University of Toulouse, Toulouse Business School (TBS), Associate Member of the Institut de Recherche en Droit Européen International et Comparé [Research Institute in European, International and Comparative Law] (IRDEIC), Co-Chair of the American Bar Association Section of International Law Privacy, E-Commerce, and Data Security Committee.

** Junior Member of the Institut Universitaire de France and a full Professor at the Université Toulouse 1 Capitole (UT1), Co-Director of the Master in Digital Law at UT1 and Assistant Director of the IRDEIC.

forgotten" internationally and propose a taxonomy. This work will allow for a determination on whether there is a convergence of norms regarding the "right to be forgotten" and, more generally, with respect to privacy and personal data protection laws. Finally, this paper will provide certain criteria for the relevant rights and organize them into a proposed analytical grid to establish more precisely the proposed taxonomy of the "right to be forgotten" for the use of scholars, practitioners, policymakers, and students alike.

INTRODUCTION

This study begins by setting out the legal context and definition of the so-called "right to be forgotten" prior to making explicit the stakes involved in this right (or really, these rights) and setting out the basis for legal taxonomies and the methodology of this paper.

A. Legal Context and Definition of the "Right to Be Forgotten"

Former European Commission Vice President and Commissioner for Justice Viviane Reding described the "right to be forgotten" as allowing an individual to obtain removal of his or her personal data from a data controller's system if there is no longer a "legitimate reason" for retaining it.[1] Conversely, American privacy scholar Jeffrey Rosen described it as "the biggest threat to free speech on the Internet in the coming decade."[2] Rather than arbitrating this dispute, this paper begins with a discussion of why and how this "right to be forgotten" has come to be so talked about, providing its legal context. After that, it hazards an initial attempt at defining the "right to be forgotten" term generally, which is not entirely useful, as many different forms of rights are now hidden behind that term.

1. Viviane Reding, Vice President and Comm'r for Justice, Fundamental Rights, and Citizenship, Eur. Comm'n, Keynote at the DLD12 Conference: All You Need Is…Data?: The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 22, 2012), http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

2. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (Feb. 13, 2012).

1. Legal Context

Perhaps one of the first times mention is made of a "right to be forgotten" in English can be found in a 1974 law review article detailing an involuntarily-committed person's only right remaining after commitment proceedings.[3] Obviously, that right has nothing to do with the right today in the context of the Internet, except that it involved what Justice Cooley, cited by Warren and Brandeis, called, almost a century earlier, the right "to be let alone."[4] For the true sources of the "right to be forgotten," as we know it today, one must look at the genesis of European privacy law, which has been described as an aspect of dignity in Western Europe.[5] This has been said to entail a "right of individual consent . . . that later evolved into the individual's right to participate in society."[6]

In Europe the "right to be forgotten" arose out of concepts of "fundamental rights," such as the "right to respect for private and family life" memorialized in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such rights have always been balanced against other rights, such as the rights of others.[7] Article 7 of the later Charter of Fundamental Rights of the European Union ("Charter") protects privacy,[8] while Article 8 of the Charter protects personal data as a fundamental right.[9]

It is useful to change language and look to the French term, "*le droit à l'oubli*" ("right to be forgotten" or, as it is sometimes translated, "right to oblivion") recognized by a court case (even if not labeled as such) as early as 1965.[10] One may look further back to the late 1800s in connection

3. Ross E. Campbell, Comment, *Progress in Involuntary Commitment*, 49 WASH. L. REV. 617, 640 (1974).

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

5. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155 (2004).

6. Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 356 (2015).

7. European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, 230. This Convention applies in the member states of the European Union and in the other nations of the Council of Europe.

8. Charter of Fundamental Rights of the European Union art. 7, 2000 O.J. (C 364) 1, 10.

9. *Id.* art. 8, at 10.

10. *See* 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 n.1 (2013) (listing relevant French and Italian case law). In a similar vein, Jeffrey Rosen says that "the intellectual roots of the right to be forgotten can be found in French law, which recognizes *le droit à l'oubli*—or the 'right of oblivion'—a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction." Rosen, *supra* note 2, at 88.

with a prohibition of certain publicity for specified judicial proceedings,[11] under the French Act of July 29, 1881,[12] sometimes known as the "Law on the Freedom of the Press." Professor Rolf Weber asserts that although a specific digital right to be forgotten has only recently been proposed, its inherent background concept has been debated for years. As an example, he cites "concerned persons who were convicted in court and who wanted to make this information disappear after a certain time period had elapsed."[13] He continues by indicating that in Europe the right may be contained within the scope of "the right of personality."[14]

On the other side of the Atlantic, Professor Franz Werro suggested in 2009 that the nearest American law had to a "right to be forgotten" was "public disclosure of private facts," which was included by William Prosser in the Restatement (Second) of Torts § 652D in 1977.[15]

However, of interest here is the "right to be forgotten" in the age of new information and communication technologies, particularly Internet and digital technologies. In France, for example, a key event in this context was the adoption of the French Data Protection Act;[16] and in Europe, generally, the adoption of the Data Protection Directive,[17] and its implementation into Member State national law,[18] including in France

11. *See* Nathalie Mallet-Poujol, *Information judiciaire et droit à l'oubli* [Judicial Inquiry and the Right to Be Forgotten], 48 LEGICOM 111, 112 (2012). Mallet-Poujol's article, which is focused on media coverage of judicial matters, concludes that the right to be forgotten is an exception with respect to the professional media, not the rule, but when farther in time from the event, a publication of the event must be of general interest—which is easier to find when a public figure is involved—in order to avoid application of the right. *Id.* at 124.

12. *See Loi du 29 juillet 1881 sur la liberté de la presse* [Act of July 29, 1881 on the freedom of the press], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 30, 1881, p. 4201, art. 39 (Fr.).

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

14. *Id.* at 121.

15. Franz Werro, *The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash*, *in* HAFTUNGSRECHT IM DRITTEN MILLENNIUM [LIABILITY IN THE THIRD MILLENNIUM] (Aurelia Colombi Ciacchi et al. eds., 2009) 285, 292 (Ger.).

16. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of Jan. 6, 1978 on Information Technology, Data Files, and Civil Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, p. 227, http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (English translation) [hereinafter French Data Protection Act].

17. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter EU Data Protection Directive].

18. Under the Treaty Establishing the European Community, as in force at the date of the adoption of the Data Protection Directive, it was left up to the "national authorities" of the Member States to choose the "form and methods" of the implementation of directives. Treaty Establishing the European Community art. 189, 1992 O.J. (C 224) 1, 65. This is also true under Article 288 of the current Treaty on the Functioning of the European Union. Consolidated Version of the Treaty on the Functioning of the European Union art. 288, 2008 O.J. (C 115) 47, 171–172 [hereinafter TFEU].

through the adoption of the Act of August 6, 2004,[19] which amended the French Data Protection Act. In *Google Spain*, the "right to be forgotten" is based on, *inter alia*, Articles 12(b) and 14(a) of the Data Protection Directive.[20]

The issue came to be widely debated both around the date of the publication of the European Commission's proposal for a General Data Protection Regulation ("GDPR") in 2012—the final adopted version of which will replace the Data Protection Directive in May 2018 and includes a "right to erasure ('right to be forgotten')"[21]—and at the time of the *Google Spain* ruling in 2014. However, other jurisdictions have seen similar developments, which shall be explored below.

Ever since the *Google Spain* ruling of the Court of Justice of the European Union ("CJEU") on May 13, 2014,[22] in which a form of "right to be forgotten" was applied, the so-called "right to be forgotten" has been at the heart of legal debate in the data protection/privacy sphere,[23] *inter alia*, including in non-English legal journals in Continental European nations.[24] As a result of the ruling in that case, Google was required to

19. Loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Act No. 2004-801 of Aug. 6, 2004 relative to the Protection of Individuals with regard to the Processing of Personal Data amending the French Data Protection Act], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Aug. 7, 2004, p. 14063 [hereinafter Act of Aug. 6, 2004].

20. *See* Case C-131/12 Judgment of the Court (Grand Chamber), Google Spain SL v. Agencia Española de Protección de Datos, CURIA paras. 89–99 (May 13, 2014) (ECLI:EU:C:2014:317), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131; *see also* W. Gregory Voss, *The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation*, 18 J. INTERNET L. 3, 4 (2014). Article 14 (a) applies in the cases referred to in Article 7 (e) and (f) of the Data Protection Directive.

21. Regulation 2016/679 of 27 April 2016 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) [hereinafter GDPR]. *Cf. 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)*, art. 17, at 51–53, COM (2012) 11 final (Jan. 25, 2012) (the proposed GDPR).

22. Case C-131/12 Judgment of the Court (Grand Chamber). For additional discussion of this case, see *infra* Section I(B)(1)(a).

23. Numerous articles have been published both on this case and on the "right to be forgotten" since the ruling was rendered. *See, e.g.*, Anna Bund, *The Curious Case of the Right to Be Forgotten*, 31 COMPUTER L. & SEC. REV. 336 (2015). *See also* David Lindsay, *The 'Right to be Forgotten' by Search Engines Under Data Privacy Law: A Legal Analysis of the Costeja Ruling*, 6 J. MEDIA L. 159 (2014); Rustad & Kulevska, *supra* note 6; Lawrence Siry, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, 103 KY. L.J. 311 (2014); Rolf H. Weber, *On the Search for an Adequate Scope of the Right to Be Forgotten*, 6 J. INTELL. PROP., INFO. TECH. & ELECTRONIC COM. L. 2 (2015).

24. *See, e.g.*, Ana Azurmendi, *Por un «derecho al olvido» para los Europeos: Aportaciones Jurisprudenciales de la Sentencia del Tribunal de Justicia Europeo del Caso*

remove certain pages of a Barcelona-based newspaper—*La Vanguardia*—regarding a judicial sale to satisfy an individual's debts to the social security system from its search results for that individual, years after the sale had occurred.[25] The CJEU found that the Data Protection Directive applied to the U.S.-based company, and that a right to object to such processing may lead to a case-by-case balancing of rights and interests in the handling of requests from data subjects exercising this right.[26]

Following the *Google Spain* ruling, Google set up an online form for receiving requests to exercise this right.[27] As of April 2, 2016, Google reported having received 411,633 delisting requests and having deleted 519,733 search engine result links, out of a total of 1,434,552 URLs examined following requests coming from all of the 28 nations of the European Union ("EU"), in addition to Iceland, Liechtenstein and Norway from the European Economic Area, as well as Switzerland.[28] The *Google Spain* ruling has been widely commented upon in the U.S. and Europe.[29]

The "right to be forgotten" had already been a subject of legal discussion for several years prior to that court ruling;[30] however, the term—which is not so much about forgetting as about delisting, deleting, erasing, and taking down—has been applied to various forms of rights,

Google Spain y su Recepción por la Sentencia de la Audiencia Nacional Española de 29 de Diciembre de 2014 [*In Support of a "Right to Be Forgotten" for Europeans: Jurisprudential Contributions of the European Court of Justice's Sentence in the Google Spain case and Their Reception by the Spanish Audiencia Nacional's Ruling of December 29, 2014*], REVISTA DE DERECHO PÚBLICO, 273 (Jan.–Apr. 2015) (Spain); *see* Gemma Minero Alejandre, *A vueltas con el «derecho al olvido». Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital* [*Going on about the "Right to be Forgotten": Legislative and Case Law Construction of the Right to Personal Data Protection in the Digital Context*], 30 REVISTA JURÍDICA UNIVERSIDAD AUTÓNOMA MADRID 129 (2014); *see also* Céline Castets-Renard, *Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique* [*Google and the Obligation to Delist Links to Personal Data or How to Be Forgotten by the Digital World*], 106 REVUE LAMY DROIT DE L'IMMATÉRIEL 68 (2014).

25. Case C-131/12 Judgment of the Court (Grand Chamber), para. 98.

26. *See generally id.*

27. *See Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited May 2, 2016).

28. *See European Privacy Requests for Search Removals*, GOOGLE TRANSPARENCY REP., https://www.google.com/transparencyreport/removals/europeprivacy/ (last visited May 2, 2016).

29. See sources cited *supra* notes 23 and 24.

30. *See, e.g.*, Matthew N. Kleiman, Comment, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1218 (1992) (mentioning the French "right to be forgotten" under national law); Karen Eltis, *Breaking Through the "Tower of Babel": A "Right to Be Forgotten" and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics*, 22 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 69, 84–89 (2011).

which are not identical.[31] The general use of the term is misleading;[32] it has resulted in legal scholars, legislators, professionals and students alike, attempting to propose definitions for the term or its counterpart "the right to oblivion."[33]

2. Definition

According to Professor Cécile de Terwangne in her article on the "right to be forgotten," "[t]he development of information and communication technologies has been a determining factor as regards extending the scope of that right."[34] However, what we call the "right to be forgotten" actually encompasses several rights to which different legal norms may apply. In addition, one may wonder if it really is possible to "forget" in this digital age, and whether all that one can really aspire to is a right to deletion of personal data concerning oneself.[35]

According to Professor de Terwangne, "[t]he right to oblivion, equally called right to be forgotten, is the right for natural persons to have information about them deleted after a certain period of time."[36] Thus, we have come back to the dilemma between forgetting as contrasted with deletion.

31. These various forms are detailed in Section I, *infra*.

32. As stated in a House of Lords report issued after the Google Spain ruling: "[t]he expression 'right to be forgotten' is misleading. Information cannot be deliberately 'forgotten'. It cannot be 'consigned to oblivion' (the expression used by the Spanish court in its request for a preliminary ruling)." EUROPEAN UNION COMMITTEE, EU DATA PROTECTION LAW: A 'RIGHT TO BE FORGOTTEN'?, 2014–15, HL 40, ¶ 15 at 9. Author Paul Bernal has complained about the name "right to be forgotten" in his blog, indicating that this has angered others, as well. He contrasts the name with that of the "right to delete" in the proposed GDPR, remarking, regarding the "right to be forgotten," that "the connotations of the name of the right as well as the implications of its implementation are of concern and have been subject to criticism. A right to be forgotten looks like the rewriting or erasing of history, or a kind of censorship." *See* Paul Bernal, *A Right to Delete – Not a Right to Be Forgotten. . .*, PAUL BERNAL'S BLOG (Aug. 7, 2014), https://paulbernal.wordpress.com/2014/08/07/a-right-to-delete-not-a-right-to-be-forgotten/. Moreover, perhaps the difficulties with the term itself are the reason why it is so often used between quotation marks and often prefaced by "so-called."

33. *See, e.g.*, Robert Kirk Walker, Note, *The Right to Be Forgotten*, 64 HASTINGS L.J. 257, 274 (2012). *See also* Mélanie Clément-Fontaine and Rafael Amaro, *Séance 9: Le droit à l'oubli numérique* [*Ninth Session: The Digital Right to Be Forgotten*], in LA PROPOSITION DE RÈGLEMENT EUROPÉEN RELATIF AUX DONNÉES À CARACTÈRE PERSONNEL : PROPOSITIONS DU RÉSEAU TRANS EUROPE EXPERTS [THE PROPOSAL FOR A EUROPEAN REGULATION ON PERSONAL DATA: PROPOSALS OF THE TRANS EUROPE EXPERTS NETWORK] 422, 424–425 (Nathalie Martial-Braz ed., Société de Législation Comparée, 2014) (Fr.) (citing definitions of the European Commission, French national assemblymen Bloche and Verchère, and the French Minister of Justice for the equivalent French terms, "*droit à l'oubli*" [right to be forgotten] or "*droit à l'oubli numérique*" [digital right to be forgotten]).

34. *See* Cécile de Terwangne, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, 13 REVISTA DE INTERNET, DERECHO Y POLÍTICA 109, 110 (2012).

35. *See generally* Paul A. Bernal, *A Right to Delete?*, 2 EUR. J.L. & TECH., no. 2, 2011.

36. *See* de Terwangne, *supra* note 34, at 110.

Obviously, the "right to be forgotten" is linked with the notion of "Internet privacy," and the meaning of the latter is sometimes unclear and its interpretation different, for example, in the U.S. and in Europe, just as is the underlying concept of "privacy" itself.[37] In the words of Professor James Whitman, "[c]ontinental law is avidly protective of many kinds of 'privacy' in many realms of life, whether the issue is consumer data, credit reporting, workplace privacy, discovery in civil litigation, the dissemination of nude images on the internet, or shielding criminal offenders from public exposure."[38] This contrasts with the U.S., which has an approach inherited from its eighteenth century history and focuses on protecting one's home, in particular, from government intrusion, which provides American privacy law with "a distinctive coloration."[39] European law may be derived from the French "right of oblivion" and what we call a "right to rehabilitation" provided to convicted criminals who have served their time. In the U.S., by contrast, "publication of someone's criminal history is protected by the First Amendment."[40]

The term "data protection" is often used to describe privacy in Europe. According to Professors Daniel Solove & Paul Schwartz, that term "reflects the modern concept of privacy protection that emerged in the 1970s as computer systems were increasingly used to process information on citizens," however, "a concept of 'privacy,' sometimes referred to as that of private life or the private domain, continues to play an important role in the European conception of information privacy."[41]

After identifying certain difficulties in defining a term that has really become a confusion of distinct rights, this paper turns to the stakes involved in the "right to be forgotten."

B. Stakes Involved in the "Right to Be Forgotten"

The importance of the "right to be forgotten" today relates directly to changes to the concept of memory: fleeting in the time before the Internet; all too permanent with the use of new technologies. Thus, this paper's discussion of the stakes of this right begins by dealing with the memory/forgetting dichotomy. Then, this paper briefly explores the role of online private actors in this context, which has been highlighted in the aftermath of the *Google Spain* ruling.

37. Whitman, *supra* note 5. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1096 (5th ed. 2015) ("United States and foreign privacy regimes differ in some respects. Consider the standard description of privacy legislation in Europe as 'omnibus' and privacy law in the United States as 'sectoral.'").

38. Whitman, *supra* note 5, at 1156.

39. *Id.* at 1215.

40. Rosen, *supra* note 2, at 88.

41. SOLOVE & SCHWARTZ, *supra* note 37, at 1097–98.

1. Memory vs. Forgetting

The "right to be forgotten" issue has come to the fore as a result of the stakes involved for the privacy of individuals on the Internet. Viktor Mayer-Schönberger discusses some of these stakes in his book *Delete: The Virtue of Forgetting in the Digital Age*.[42] The concerns of individuals range from the security of their personal data, to the fact that once such data are out on the Internet they remain there (e.g., embarrassing photographs on social networks),[43] to the dangers this may potentially pose for their careers, their relationships, and perhaps their identity (including financial account information subject to identity theft). A Pew Research Center study found that "Americans' perceptions of privacy and their sensitivities about different kinds of personal information are varied, but their lack of confidence in the security of digital communications channels is universal."[44] This lack of trust also has a negative effect on online services, as pointed out by the European Commission, when it proposed to deal with cybersecurity and personal data protection in order to promote the use of online services within the framework of its Digital Agenda.[45] Focusing more on the individual, Google's Eric Schmidt and Jared Cohen said:

> It's because of data permanence that we think twice before posting a photo, or check that a connection is secure before entering a password, or ponder whether an offhand comment on a message board might raise the eyebrows of a would-be employer in twenty years. Who would have guessed that parents need to talk about all of this with their children, all of the issues related to preserving privacy and security online, before they even have the first conversation about sex? Yet this is the world we live in, in which data cannot be put back in the box.[46]

Individuals' concerns about online privacy may be exacerbated by their loss of control once material is published online, especially where search engines may store or link to past versions of webpages through

42. *See generally* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

43. Take, as an example, the case of Stacy Snyder, the "young teacher-in-training," who put a photo of herself as "Drunken Pirate" on MySpace and lost her job for promoting underage drinking. *See id.* at 1–2; *see also* Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1532 (2012).

44. PEW RESEARCH CENTER, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 12 (2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

45. *See Digital Single Market Pillar III: Trust & Security*, EUR. COMMISSION, http://ec.europa.eu/digital-agenda/en/our-targets/pillar-iii-trust-security (last visited May 2, 2016).

46. ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE 273 (Vintage Books 2014).

caching.[47] Such concerns may also be more and more justified by cybersecurity threats such as those of the "Impact Team" of hackers who disclosed personal information gleaned from hacking into dating websites, including the Ashley Madison site.[48] This concern may be heightened by the sensitive nature of the data—in the European sense of sensitive data (which if disclosed might harm the user, such as through discrimination)[49]—contributed by the users of such websites, as France's data protection agency has aptly pointed out.[50] The issue has arisen from the desire of the individual to "determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."[51]

Consistent with the ideas of Mayer-Schönberger, Professor de Terwangne contrasts human and digital memory:

> The infallibility of the "total memory" of the Internet contrasts with the limits of human memory. Now memory can be one of rancor, vengeance or belittlement, thanks to the "eternity effect" of the Internet, which preserves bad memories, past errors, writings, photos and videos we would like to deny at a later stage.[52]

The balance at stake—at the heart of the "right to be forgotten" or to "oblivion"—is one referred to again and again: between "free dissemination of information" and "individual self-determination."[53]

A little more than a year prior to proposing the GDPR, Viviane

47. For a short discussion of search engine caching and the difficulties for website owners to remove content from the web because of search engine practices, *see* Emily B. Laidlaw, *Private Power, Public Interest: An Examination of Search Engine Accountability*, 17 INT'L J. L. & INFO. TECH. 113, 140–141 (2009).

48. Ashley Madison, owned by Avid Life Media, is a "popular online dating service marketed to people trying to cheat on their spouses." Dino Grandoni, *Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions*, N.Y. TIMES (Jul. 20, 2015), http://nyti.ms/1KgUFLl. It announced in July 2015 that hackers had breached its site and may have obtained members' personal data. *Id.* The hackers said that they had obtained information on thirty-seven million of the site's members. *Id.* Two other websites owned by the same company as Ashley Madison—Cougar Life and Established Men—were also hacked. *See id.*

49. EU Data Protection Directive, *supra* note 17, at 40 ("personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life").

50. *See* Commission nationale de l'informatique et des libertés [CNIL] [National Commission for Data Protection Authority], *Sites de rencontre en ligne: comment protéger votre intimité?* [*Online Dating Sites: How to Protect Your Privacy?*], CNIL.FR (Jul. 28, 2015). The CNIL gave formal notice to eight dating website owners (with respect to thirteen websites) to take action within a three-month period to make their websites compliant with data protection law or face sanctions. *See* CNIL, *Données traitées par les sites de rencontre: 8 mises en demeure* [*Data Processed by Dating Sites: Eight Formal Notices Issued*], CNIL.FR (Jul. 28, 2015).

51. Mantelero, *supra* note 10, at 230.

52. de Terwangne, *supra* note 34, at 110.

53. *Id.*

Reding commented that "[w]ith more and more private data floating around the web—especially on social networking site [sic]—people should have the right to have their data completely removed."[54] Reding's words highlight the impact the "right to be forgotten" has on the freedom of expression, and the risk that it may pose to the quality of information contained on the Internet, if it is used to censor or for "rewriting history."[55] Nonetheless, the European Commission has argued that there is no such risk, all the while highlighting certain areas where risks had been identified by others—the press and media, history, scientific research, and archives:

> The right to be forgotten is not about rewriting history. The Commission's proposal protects freedom of expression and the freedom of the media, as well as historical and scientific research. It provides exemptions for these sectors asking Member States to adopt national laws to guarantee the respect of these fundamental rights. This allows archives to continue operating on the basis of the same principles as today. . . . *In short, the right to be forgotten is not absolute and does not affect historical research or the freedom of the press.*[56]

In addition, there is another risk coming from concerns about national security, which many people link with privacy. Though this paper will not develop this point further, it is worth mentioning.[57] Another area to explore is the role of private actors in connection with the "right to be forgotten."

2. Role of Private Actors

Search engines also play another role in this context. As mentioned by the CJEU in the *Google Spain* case (speaking of personal data published on websites):

> [I]t is undisputed that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data

54. Viviane Reding, Vice-President and Comm'r for Justice, Fundamental Rights, and Citizenship, Eur. Comm'n, Speech at The European Data Protection Privacy Conference: Creating a Modern and Harmonized Regulatory Framework, Privacy Matters – Why the EU Needs New Personal Data Protection Rules (Nov. 30, 2010), http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm.

55. *See, e.g.*, Rustad & Kulevska, *supra* note 6, at 369. The authors point out that since the "right to be forgotten" does not generally distinguish between true and false information, data controllers are "in the unenviable position of effectively rewriting history."

56. European Commission Press Release IP/14/60, Data Protection Day 2014: Full Speed on EU Data Protection Reform (Jan. 27, 2014) (emphasis in original).

57. For a critical analysis, see generally DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011). Here "security" indicates national security. Note that in data protection law there is also a linked concern with another kind of security—that of data processing. *See, e.g.*, EU Data Protection Directive, *supra* note 17, at 43.

> subject's name, including to internet users who otherwise would not have found the web page on which those data are published.[58]

Reportedly, the individuals who have manifested concern through Google "right to be forgotten" requests are "ordinary individuals,"[59] meaning that search engines—as Internet intermediaries—are now being solicited in the regulation of the Internet.[60] This role in regulating the Internet may be deduced from Google's exercise in conducting hearings throughout Europe in order to obtain advice on the handling of requests for the exercise of the rights recognized in *Google Spain*, resulting in a report by its so-called "Advisory Council."[61] Although its rulings may be "appealed" to EU Member State data protection agencies and courts, Google acts in these cases somewhat like a judge assessing the merits of requests. Professor Weber would concur, and has highlighted that, as a result of *Google Spain*, "search engines do have wide discretion in the decision-making about submitted requests to have certain links deleted, thereby executing the function of a judge."[62] On another front, Internet intermediaries have been solicited in the fight against terrorism through online channels, for example, after the *Charlie Hebdo* attacks in Paris in January 2015.[63]

C. Basis for Legal Taxonomies and Methodology

Legal taxonomies exist in various frameworks, and furthermore, there are advantages in identifying aims and methodologies prior to developing this subject further. This section sets forth (1) a discussion of methodology and (2) a development of the aims of this study.

58. *See* Case C-131/12 Judgment of the Court (Grand Chamber), Google Spain SL v. Agencia Española de Protección de Datos, CURIA para. 36 (May 13, 2014) (ECLI:EU:C:2014:317), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ013.

59. One article reported that 95% of Google "right to be forgotten" requests are from "citizens out to protect personal and private information—not criminals, politicians and public figures." Sylvia Tippman & Julia Powles, *Google Accidentally Reveals Data on 'Right to Be Forgotten' Requests*, GUARDIAN (Jul. 14, 2015, 9:28 AM), http://gu.com/p/4a9hc/stw.

60. For some of the ways in which intermediaries are involved, see Marvin Ammori, *Recurring Myths About the Legal Obligations of Online Platforms*, CTR. FOR INTERNET & SOC'Y (Sept. 5, 2013, 9:36 AM), http://cyberlaw.stanford.edu/blog/2013/09/recurring-myths-about-legal-obligations-online-platforms.

61. *See, e.g.*, LUCIANO FLORIDI ET AL., REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN (Feb. 6, 2015), https://www.google.com/advisorycouncil/.

62. *See* Weber, *supra* note 23, at 8.

63. *See, e.g.*, Olga R. Rodriguez, *French Minister Meets with Google, Facebook, Twitter*, DENVER POST (Feb. 21, 2015, 12:32 AM), http://dpo.st/1DDAZQX.

1. Methodology

In the legal context, taxonomy has been described by Professor Ugo Mattei of Hastings as "the grammar of the legal discourse," allowing discussion between lawyers.[64] In the context of a "world of legal globalization," Professor Mattei also sees global taxonomy as something necessary.[65] Various legal actors engage in legal taxonomy on an ongoing basis "sorting the law into classes as they discuss and apply it."[66] Professor Emily Sherwin of Cornell indicates that this sorting may be with respect to "posited rules" (those whose meaning is established by the maker of the rules), "attributed rules" (e.g., those attributed by the author to prior decision, legislative rules, or legal materials), and "ideal rules" (where nothing has been posited by an authority, but which reflect the author's "best imaginable set of rules to govern conduct and decision").[67]

Professor Sherwin then defines five criteria for classifying law—"intuitive similarity," "evolutionary history," "formal classification," "function-based classification," and "reason-based classification"[68]—and then determines that only the latter three are "plausible methods for classifying law."[69]

The methodology of this paper involves an analysis of Professor Sherwin's second level of subject matter—attributed rules: organizing rules derived from prior rulings, rules, and materials. This analysis is made necessary by the ambiguity created by the use without standard definition or classification of different terms such as "the right to be forgotten," "the right to erasure," "the right to oblivion," and so on. This paper makes no attempt to define an ideal rule, but analyzes what now exists.

With respect to the criteria of classification, this paper also rejects intuitive similarity, based on what Sherwin refers to in part as "emotional responses to the subject matter,"[70] and discounts evolutionary history as a criterion. Of Sherwin's remaining three criteria, that which seems to be the most germane is the function-based taxonomy, "which sorts legal rules according to the types of controversies they are designed to resolve and

64. *See* Ugo Mattei, *Three Patterns of Law: Taxonomy and Change in the World's Legal Systems*, 45 AM. J. COMP. L. 5 (1997). Professor Mattei's analysis is placed at a higher level of classification—that of legal systems—nonetheless, his general comments on taxonomy are of interest.

65. *Id.* at 6. It also should be added that this global view will help achieve what one author has referred to as "a cosmopolitan understanding of privacy law," here with respect to the "right to be forgotten," and "trans-systemic thought." *See* Eltis, *supra* note 30, at 74.

66. Emily Sherwin, *Legal Taxonomy*, 15 LEGAL THEORY 25, 27 (2009).

67. *Id.* at 28–31.

68. *Id.* at 31–39.

69. *Id.* at 39.

70. *Id.* at 31.

thus reflects the different roles legal rules play in society."[71] These types of controversies may be elicited by various means, which will be addressed in this paper.

Sherwin also refers to different purposes of classification. This paper favors what she considers the "most basic and least ambitious goal," which is to organize a body of law for "ease of use," although this is the category that she most associates with formal taxonomy, rather than the functional one selected for this paper.[72] In this sense, this paper fits within the aspiration that she describes as contributing to "the lucidity of legal thought and the quality of legal decision-making."[73]

Paradoxically, to the authors' knowledge, little previous general effort at categorization has been made specifically with respect to the "right to be forgotten," unlike the area of privacy, generally,[74] or privacy torts, specifically,[75] or other areas of law.[76]

There is a dearth of literature critically describing the various forms of the "right to be forgotten," with one notable exception that this paper discusses further below. Nonetheless, one recent article set out various forms of an erasure right under the term "the three degrees of deletion."[77] These degrees of deletion—which may be seen as a sub-subset of what has been described as the "right to be forgotten"—give data subjects the right to take down certain materials from the Internet, and are described as follows:

- First degree: "Data subject's own postings and pictures online";
- Second degree: "Data subject posts content that a third party copies and reposts on the third party's own site"; and
- Third degree: "Third party posts data not created by the data subject but that is about the data subject."[78]

71. *Id.* at 39.

72. *Id.* at 40.

73. *Id.*

74. In facing up to "a concept in disarray"—namely, privacy—where "[n]obody can articulate what it means," one privacy scholar's dilemma was much the same as that of this paper. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

75. Professor Solove recalls William Prosser's "four types of harmful activities redressed under the rubric of privacy:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness,"

which served as a narrower privacy taxonomy. *Id.* at 482–483 (citing William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960)).

76. In the area of environmental law, see, for example, Todd S. Aagaard, *Environmental Law as a Legal Field: An Inquiry in Legal Taxonomy*, 95 CORNELL L. REV. 221 (2010).

77. Rustad & Kulevska, *supra* note 6, at 387–98.

78. *Id.* at 389. These three categories are largely the same as those mentioned by then

Although these classifications are helpful, they are far from comprehensive.[79] Moreover, such discussion, limited itself to the U.S. and the EU, focused on the *Google Spain* Case and failed to analyze other forms of the "right to be forgotten." In addition, these categories do not comment directly upon the "right to be forgotten" but merely upon one of its subsets—a right to deletion—and then only upon the context in which it is exercised. As a result, it is more a description of the various contexts in which one of the aspects of the "right to be forgotten" is implemented. This is all the more reason for us to continue our task.

In addition, and more importantly, prior to the *Google Spain* case, Professor de Terwangne set out and analyzed three different categories of the "right to be forgotten/right to oblivion": "the right to oblivion of the judicial past, the right to oblivion established by data protection legislation and a new, and still controversial, digital right to oblivion that amounts to personal data having an expiration date or being applicable in the specific context of social networks."[80]

While these categories seem very pertinent, this paper has taken a more comparative view, classifying existing law with a more international perspective—considering law beyond the U.S. and the EU, as well. As such, this study could be seen as building upon the work of de Terwangne, but taking her work a step further by developing a coherent taxonomy for truly international use. Additionally, this paper benefits from a post-*Google Spain* viewpoint. This means that de Terwangne's third "new, still controversial, digital right to oblivion" has taken on substance since the time of her writing, and this paper also benefits from this new vantage point in its study. Furthermore, this paper's classification has been refined with developments in U.S. law, and the last of de Terwangne's rights to oblivion has been divided into three, as legal norms have become more precise. But what binds the two halves together is the digital context in which they arise and are applied, which is generally lacking in her first two categories regarding oblivion in connection with the judicial past and as provided by data protection legislation. So, this paper will now introduce its basis for a legal taxonomy of the various forms of rights hidden behind that term, and survey the international legal instruments providing such rights, which helped guide the establishment of the

Google chief privacy counsel in a blog post. *Cf.* Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PRIVACY. . . ? (Mar. 9, 2011, 8:59 AM), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html, *cited in* Rosen, *supra* note 2, at 89–91.

79. This may remind one of Solove's concern with Prosser's four categories of privacy torts: "Prosser only focused on tort law. American privacy law is significantly more vast and complex." *See* Solove, *supra* note 74, at 483.

80. *See* de Terwangne, *supra* note 34, at 109.

taxonomy.

2. Aims of this Study

This study has as its central hypothesis that in order to understand these various forms of rights, above and beyond a single definition of a "right to be forgotten," an international survey of the "right to be forgotten" must be undertaken and a legal taxonomy developed so that scholars compare similar rights—apples with apples and oranges with oranges, so to speak. Moreover, thanks to the example of the "right to be forgotten," this article seeks to study whether there is a convergence of norms on privacy and personal data protection laws. Particularly, it considers the real influence of European law on this topic. We usually say that the Data Protection Directive has served as a model for many pieces of legislation on data protection laws around the world but this paper's aim is to attempt to measure in qualitative manner the real impact of the European values underpinning this legislation.

This paper endeavors to fill this gap in the literature by proposing a taxonomy for the "right to be forgotten," before providing an international survey of the forms of this right and a study of the convergence of norms. In doing so, it does not propose to deal with means other than legal norms—or "privacy rights" created by law (whether statute or case law). Thus, this paper will not enter into discussions of technical protections—such as "privacy DRM"—nor is it intended to deal with practices such as "digital abstinence," which constitute potential responses to privacy threats which arise from the use of digital technology and are amply set out by Mayer-Schönberger.[81] Below, Section I develops the "right to be forgotten" further, including some of its sources.

I. INTERNATIONAL SURVEY OF FORMS OF THE "RIGHT TO BE FORGOTTEN"

This section reviews the international legal instruments that this paper considers in distilling its taxonomy. The rights reviewed will come from many different jurisdictions in order to obtain a comparative view—consistent with this paper's position on attributed rules—of what legislation and court rulings exist, and what additional rules may soon come into being. All the while, this paper measures the extent of "legal globalization" in the matter, including the impact of the *Google Spain* case, which this paper believes further proves the need for such taxonomy, consistent with the view of Professor Mattei. This paper proceeds as follows: first it specifies the forms of the "right to be forgotten" that have been identified, dividing examples of such rights from various nations

81. *See* MAYER-SCHÖNBERGER, *supra* note 42, at 128–168.

worldwide into these categories, prior to discussing whether these different examples indicate that there is an international convergence of legal norms. Thus, this paper begins with its categories of the "right to be forgotten."

This paper details five main types of rights to be forgotten, three of which are similar to those proposed by Professor de Terwangne and set forth above, and two of which, the fourth and fifth, are nascent rights which the paper has chosen to treat together (in each case, the proposed short name of each type is indicated in italics and bold):[82]

1. ***Right to rehabilitation***: the right to oblivion of the judicial past;
2. ***Right to deletion***/erasure: the right to oblivion established by data protection legislation;
3. ***Right to delisting***/delinking/de-indexing;
4. ***Right to obscurity*****;** and
5. ***Right to digital oblivion*** of data collected by information society services.

The first two rights listed above are old and not linked to the digital age, in contrast to the last two rights listed, which appeared later in a digital context. The fifth one is a "digital right to oblivion that amounts to personal data having an expiration date or being applicable in the specific context of social networks."[83] Nonetheless, the third right is relatively recent, but is based on the foundation established by this paper's second category of rights, which is older and developed prior to the digital age. In fact, one could say that a new and audacious interpretation of the second right—as in the case of *Google Spain*—led to a new third right (or at least to a remarkable extension of the existing second right).

Since the CJEU's *Google Spain* case recognized a right to delisting, this paper is able be more precise. It is a form of digital right to oblivion with respect to search results referencing a natural person. In addition, other forms of similar rights may be observed. Indeed, the analysis undertaken in this study discovered that in the U.S., it may be easier to recognize a right to obscurity rather than a right to delisting in the digital context. That is why this paper proposes a distinction between the fourth

82. *See supra* Introduction, section A.1. "Information society service" is the term used in Europe, under EU law, to refer to "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 Amending Directive 98/34/EC Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations, 1998 O.J. (L. 217) 18, 21 art. 1(2)(a)(2).

83. *See* de Terwangne, *supra* note 34, at 109. This paper notes that this concept of an informational expiration date as a means to reintroducing "forgetting" in the digital context (or, as Mayer-Schönberger puts it, to "mimic human forgetting in the digital realm") is well developed by Mayer-Schönberger. *See* MAYER-SCHÖNBERGER, *supra* note 42, at 171–195.

and fifth rights. Moreover, a real "right to be forgotten" of the data collected by information society service providers or operators appears with the GDPR. Thus, with the advantage of both hindsight and knowledge of subsequent developments, this paper is able to fine-tune Professor de Terwangne's taxonomy with respect to this point, because with the knowledge of today, the concept of digital oblivion can be further clarified.

This paper presents an international survey of the "right to be forgotten," organized according to the form of such right (taken from the list of the proposed taxonomy) that is present in each case, in a general context and in a digital context.

A. The "Right to Be Forgotten": General Context

In this section, this paper analyzes the first two of our categories of the "right to be forgotten," which existed prior to the digital age: (1) the right to rehabilitation (right to oblivion of the judicial past), and (2) the right to deletion or erasure (right to oblivion provided by data protection regulation). These constitute the rights in the general context, prior to the digital context.

1. *Right to Rehabilitation*: Right to Oblivion of the Judicial Past

The right to rehabilitation guarantees a right to social reintegration after a judicial conviction. It is the right to oblivion of the judicial past. It recognizes that under certain circumstances it may be appropriate to grant a pardon to a person who has been convicted of a criminal offense, after a certain period of time following such conviction and after such person, who has evidenced good behavior, has served his or her sentence. This right is present in Europe, as well as outside of Europe. This paper will commence with examples from France, the United Kingdom, and the United States.

a. France

French law recognizes the right to rehabilitation in Article 133-12 of the French Penal Code. That Article provides that:

> Any person punished by a sentence for a felony, misdemeanour or petty offence is entitled, either to a rehabilitation as of right pursuant to the conditions set out in this article, or to a rehabilitation order made pursuant to the conditions contained in the Code of Criminal

> Procedure.[84]

According to one author, this right is limited to cases where strict conditions are met:

> The conditions for judicial rehabilitation are extremely strict, which coheres with the very reasons underpinning this action: the ex-offender must indeed have totally desisted from crime; he must also have been "doing good" by becoming a nearly perfect citizen.
>
> This being said, the scope of judicial rehabilitation is one of the largest of all: it can apply to all types of sentences, custody included, and all types of offences, even to the most serious ones, which are labelled "crimes" in the French legal system.
>
> Only a sentence passed by a French court can naturally be rehabilitated.[85]

Thus, although the right to rehabilitation is a broad right in France, in the context of judicial sentences, many conditions must be met in order for it to apply.

b. United Kingdom

In the United Kingdom, a right to rehabilitation also exists under a legislative act: The Rehabilitation of Offenders Act (1974)[86] allows some convictions to be ignored after the passage of a certain period of time, which period begins after the sentence has been served.[87] Its purpose is clear from the introductory words of the Act: "to rehabilitate offenders who have not been reconvicted of any serious offence for periods of years, to penalise the unauthorised disclosure of their previous convictions."[88] After a period determined by the sentence has run, if the offender has not committed another offense and been convicted of it, then generally speaking the conviction need no longer be disclosed (e.g., on job applications).

84. CODE PÉNAL [C. PÉN.] [PENAL CODE] art. 133-12 (Fr.), (John Rason Spencer QC, trans.), http://legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

85. Martine Herzog-Evans, *Judicial Rehabilitation in France: Helping with the Desisting Process and Acknowledging Achieved Desistance*, 3 EUR. J. PROB. 4, 4–19 (2011), http://www.ejprob.ro/uploads_ro/719/Judicial_rehabilitation_in_France.pdf.

86. Rehabilitation of Offenders Act 1974, c. 53 (Eng.), http://www.legislation.gov.uk/ukpga/1974/53/contents.

87. Certain serious sentences, such as those for life imprisonment, are excluded from the rehabilitation provisions of the Act. *See id.* § 5(1).

88. *Id.* at Introduction.

c. United States

In the U.S., this type of "right to be forgotten" also exists. For instance, Connecticut State law allows for erasure of records subject to certain conditions (such as the passage of time), *inter alia*, if a person is found not guilty, a case is dismissed, or nullified.[89] Other U.S. states allow for erasure of records as well.[90] This erasure allows for a person to be "rehabilitated" in the eyes of the public, for "protection to individuals with arrest or conviction records."[91]

In addition, there exists a specific U.S. Federal Act that this paper has chosen to place in this field called the Fair Credit Reporting Act ("FCRA"),[92] which aims at ensuring the accuracy and fairness of credit reporting, and regulates consumer credit reporting agencies. Under FCRA, certain information may not be provided in consumer credit reports: bankruptcy proceeding orders for relief or adjudications more than ten years before the report; suits and court judgments more than seven years old (unless the statute of limitations is longer, in which case older than that period); tax liens paid more than seven years prior to the report, etc.[93] In certain circumstances, involving high-value credit or insurance transactions, or high-salary employment, these limitations do not apply.[94] This paper considers that this is a form of right to rehabilitation, aiding social integration, even though it handles situations different from the judicial convictions covered by the other acts included in our discussion of the right to rehabilitation.

FCRA provides an opt-out provision for consumers to exercise with respect to credit or insurance transactions that they do not initiate.[95]

89. CONN. GEN. STAT. § 54-142a (2012).

90. *See* Bill Keller, *Erasing History*, N.Y. TIMES (Apr. 28, 2013), http://nyti.ms/1dhsZuB ("Most states have some version of expungement laws, or erasure laws as they are sometimes called. They are intended to let those whose cases have been dropped or overturned get on with their lives, unencumbered by the taint of arrest.").

91. *See* Linda S. Buethe, *Sealing and Expungement of Criminal Records: Avoiding the Inevitable Social Stigma*, 58 NEB. L. REV. 1087, 1088–89 (1979). Buethe's early discussion of the dangers of criminal records in an "increasingly computerized society," *id.* at 1087, highlights several State sealing or expungement statutes: Maryland (the arrestee had to petition for expungement), Nevada (the arrestee had to petition for sealing), California (with a "scattered patchwork" of expungement laws), etc. *Id.* at 1110–12.

92. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq* (1970).

93. *Id.* § 1681c(a).

94. *Id.* § 1681c(b).

95. This opt-out is necessary because under 15 U.S.C. § 1681b(a)(3), the credit reporting otherwise has the right to issue reports even where the consumer does not request the credit or insurance offer. The relevant text from 15 U.S.C. § 1681b(e)(1) follows:

> A consumer may elect to have the consumer's name and address excluded from any list provided by a consumer reporting agency under subsection (c)(1)(B) in connection with a credit or insurance transaction that is not initiated by the consumer, by notifying the agency in accordance with paragraph (2) that the consumer does not

Additional provisions allow for the blocking of information from identity theft.[96] Finally, a procedure exists to contest the accuracy of information included in a credit report and to seek deletion of inaccurate information.[97] It should be noted that FCRA was amended by the Fair and Accurate Credit Transactions Act of 2003,[98] which notably enhanced provisions already mentioned above to protect against identity theft. This right to delete is, once again, very specific and not of general application.

2. *Right to Deletion*/Erasure (or to Delete): Right to Oblivion Established by Data Protection Legislation

The right to deletion (or erasure, sometimes also expressed as a "right to delete"), as identified in this paper, is established by national data protection legislation.[99] According to Greenleaf, there were 109 privacy laws in the world in January 2015, up 10% from 99 in June 2013.[100] He notes that, "[d]ata privacy laws are clearly no longer 'a European thing,' though the influence of 'European standards' remains paramount."[101] If one considers only the right to deletion, this affirmation seems to be confirmed. However, one could also say that the right to deletion became more widespread after the establishment of the Organization for Economic Cooperation and Development ("OECD")[102] Privacy Principles contained in the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)*.[103] In paragraph 13 of the OECD Guidelines the Individual Participation Principle is set out, including the right provided to individuals "to challenge data relating to

consent to any use of a consumer report relating to the consumer in connection with any credit or insurance transaction that is not initiated by the consumer.

96. *Id.* § 1681c-2.

97. *Id.* § 1681i.

98. Fair and Accurate Credit Transactions Act of 2003 (FACT), Pub. L. 108-159 (2003), 117 Stat. 1952, (codified at 15 U.S.C. § 1601 *et seq*.).

99. For the extent of these laws' adoption worldwide, *see Data Protection Laws of the World*, DLA PIPER, http://www.dlapiperdataprotection.com/#handbook/world-map-section (last visited May 4, 2016).

100. Graham Greenleaf, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority*, 133 PRIVACY L. & BUS. INT'L REP. 1, 14–17 (2015).

101. *Id.* at 3.

102. The OECD has 34 member nations, currently including 21 out of the 28 EU Member States, Australia, Canada, Chile, Iceland, Israel, Japan, Korea, Mexico, New Zealand, Norway, Switzerland, Turkey, and the United States. *See Members and partners*, ORG. FOR ECON. COOPERATION & DEV., http://www.oecd.org/about/membersandpartners/ (last visited May 4, 2016).

103. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. COOPERATION & DEV., http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Apr. 28, 2016) [hereinafter *OECD Guidelines*]. The OECD Guidelines were updated in 2013, but we will refer to the original 1980 version.

him and, if the challenge is successful to have the data erased, rectified, completed or amended."[104]

This paper does not pretend to be entirely exhaustive in the various examples that it cites. Instead, it identifies the relevant main pieces of legislation, first by reviewing the right to deletion in greater Europe, before turning to certain nations in North America, Latin America, the South Pacific, Asia, and Africa. This paper has focused on those statutes and regulations that have an impact in the digital world, which is the highlight of this paper's concerns.

a. Europe

The Data Protection Directive applies to the European Economic Area ("EEA"), which includes all EU countries and the non-EU countries of Iceland, Liechtenstein, and Norway. Similar legislation has been enacted in Switzerland, Guernsey, Jersey, the Isle of Man, the Faeroe Islands, and Andorra. In addition, one must also consider the Council of Europe's Convention on personal data protection ("Convention 108").[105] This paper will start its analysis by looking at EU legislation.

i. European Union

The Data Protection Directive was the most important piece of European privacy legislation[106]—one which served as a model of "omnibus" privacy legislation for other countries around the world, outside of Europe.[107] In the words of Professors Solove and Schwartz:

> The Data Protection Directive establishes a basic legislative framework for the processing of personal information in the European Union. The EU Data Directive has had a profound effect on the development of privacy law, not only in Europe but also around the world.[108]

According to Professor Gregory Schaffer, there has been a "ratcheting up" effect in the relationship between the U.S. and Europe in the area of privacy policy.[109] Moreover, the sharing of data throughout the

104. *Id.* at para. 13(d).

105. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S No. 108, http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm [hereinafter Convention 108].

106. EU Data Protection Directive, *supra* note 17.

107. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 914–16 (2009).

108. SOLOVE & SCHWARTZ, *supra* note 37, at 1097.

109. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards*, 25 YALE J. INT'L L. 1 (2000).

EU encourages other nations to enact equivalent standards because an "adequate level of protection" is required by Article 25 of the Data Protection Directive in order to allow cross-border transfers of personal data to non-EU countries.[110]

Prior to the adoption of the Data Protection Directive, in the 1970s, France and Germany enacted national privacy legislation. These countries are two of the leaders in information privacy law. As stated by Professors Solove and Schwartz, "[t]he choice was also made in these key European nations to enact 'omnibus' privacy laws."[111] Indeed, the French Data Protection Act is a general privacy act.

But the Data Protection Directive's aim, which is twofold, may be considered ambiguous or even paradoxical: Its purpose is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data,"[112] while at the same time not to "restrict nor prohibit the free flow of personal data between Member States for reasons connected with" such protection.[113] Thus, it is meant to facilitate the free flow of personal data within the EU by setting an equally high privacy level in all EU Member States, while encouraging the free flow of goods and services, labor and capital,[114] a goal which harkens back to the establishment of the EU single market.

Nevertheless, since the adoption of the Treaty of Lisbon,[115] Article 16 of the Treaty on the Functioning of the European Union ("TFEU")[116] explicitly protects personal data.[117] Furthermore, the adoption of the Charter at the same time increases the citizens' protection.[118] The Charter's Articles 7 and 8 provide, respectively, that: "Everyone has the right to respect for his or her private life and family life, home and communications,"[119] and "[e]veryone has the right to the protection of personal data concerning him or her."[120] Moreover, Article 8(2) provides:

110. EU Data Protection Directive, *supra* note 17, art. 25., at 45–46.

111. SOLOVE & SCHWARTZ, *supra* note 37, at 1134.

112. EU Data Protection Directive, *supra* note 17, art. 1(1), at 38..

113. *Id.* art. 1(2), at 38.

114. *Id.* recital 3, at 31.

115. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 2007 O.J. (C 306) 1.

116. TFEU, *supra* note 18.

117. *Id.* art. 16, at 55 ("1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.").

118. *See* Charter of Fundamental Rights of the European Union, *supra* note 8.

119. *Id.* art. 7, at 10.

120. *Id.* art. 8(1), at 10.

> Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[121]

In addition, Article 8(3) adds that, "[c]ompliance with these rules shall be subject to control by an independent authority."[122] The GDPR is based on the TFEU Article 16(1) and Article 8(1) of the Charter.[123]

Now, this paper will consider the right to erasure. Article 6(1) of the Data Protection Directive requires an explicit right to erasure:

> Member States shall provide that personal data must be:
>
> . . . .
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.[124]

The French Data Protection Act, as amended to implement the Data Protection Directive, also requires an explicit right to deletion in Article 6, *inter alia*, where data are inaccurate or obsolete:

> Processing may be performed only on personal data that meet the following conditions:
>
> . . .
>
> 4° they shall be accurate, complete and, where necessary, kept up-to-date. Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and incomplete with regard to the purposes for which they are obtained and processed;
>
> 5° they shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.[125]

In the ongoing EU data protection law reform, on the occasion of the

121. *Id.* art. 8(2), at 10.
122. *Id.* art. 8(3), at 10.
123. *See* GDPR, *supra* note 21, recital 1, at 1.
124. *See* EU Data Protection Directive, *supra* note 17, art. 6(1), at 40.
125. *See* French Data Protection Act, *supra* note 16, art. 6, at 9.

proposal of the GDPR in which she introduced a "right to be forgotten," Viviane Reding highlighted the need for individuals to have control of their data and to be informed on how to delete them, adding, regarding social network sites:

> [I]f people no longer want to use a service, they should have no problem wiping out their profiles. The right to be forgotten is particularly relevant to personal data that is no longer needed for the purposes for which it was collected. This right should also apply when a storage period, which the user agreed to, has expired.[126]

Article 17 of the recently adopted GDPR also requires a "right to erasure ('right to be forgotten')," *inter alia*, when data "are no longer necessary in relation to the original purposes for which they were collected or otherwise processed," or where "the data subject withdraws consent on which the processing is based."[127] Article 19 of the GDPR adds that the "controller shall communicate any . . . erasure . . . to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort."[128] This latter proviso significantly limits the effectiveness of this right.

Even before the GDPR was proposed by the European Commission in 2012, however, concern was expressed about the practicality of a "right to be forgotten," based on its vagueness (as well as wariness that it may be used for "censorship"),[129] in addition to worries about it impacting free speech, "leading to a far less open Internet."[130]

According to Professors Solove and Schwartz, "[t]his version of the right to be forgotten raises complex questions regarding the precise obligations of the controller and downstream third parties, such as search engines and advertising networks, which have many innovative ways of collecting, tracking, and, in some cases, re-identifying data."[131] In reality, however, although this so-called "right to be forgotten" is not limited to minors, it applies in various limited cases, so it is not a general right.

Therefore, this paper concludes that it is not a true overarching "right to be forgotten," but merely the possibility to have data deleted in certain circumstances. In addition, such limited cases do not appear to differ from those already provided for in the Data Protection Directive. Indeed, the guiding data protection principles of necessity, proportionality, and purpose limitation may be used to achieve the same results, leading this

126. Reding, *supra* note 54.
127. GDPR, *supra* note 21, art. 17, at 43–44.
128. *Id.* art. 19, at 45.
129. *See, e.g.*, Fleischer, *supra* note 78.
130. *See* Rosen, *supra* note 2, at 88.
131. SOLOVE & SCHWARTZ, *supra* note 37, at 1161.

paper to determine that the GDPR does not make any major changes in this regard. In other words, as soon as the purpose limitation or consent principle is no longer respected, or the processing no longer has a legitimate basis, or the right of the data subject to object has been exercised, the relevant data should no longer be retained. In summary, this paper considers that the GDPR has not fundamentally changed the situation existing under the Data Protection Directive in this regard, and that there is no new "right to be forgotten" under the GDPR, but merely a right to have the data destroyed when they are out of date, obsolete, irrelevant, or excessive considering the purpose of the processing. Later, this paper shows that the *Google Spain* decision was more ambitious than the GDPR.

Fundamentally, however, the GDPR has the merit of emphasizing this "right to be forgotten" and making explicit that which one might have previously deduced from the guiding data protection principles, even if a "right to be forgotten" or a right to deletion of data had not expressly been mentioned beforehand. This Article of the GDPR has also been widely reported in Europe and beyond. The "right to be forgotten" enshrined in the GDPR seems of more symbolic importance than substantive effect, as soon as one goes beyond the simple statement of principle and pays attention to the conditions and modalities of its implementation.

Article 17(3) of the GDPR establishes certain limits to this right:

> Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
>
> a. for exercising the right of freedom of expression and information;
>
> b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
>
> d. for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes in accordance with Article 89(1) . . . ; or
>
> e. for the establishment, exercise or defense of legal claims.[132]

132. GDPR, *supra* note 21, art. 17(3), at 44.

The limits thus established very clearly show the balancing of interests that must be implemented when one wants to invoke the "right to be forgotten": Balancing forgetting against the "right to know," and, therefore, freedom of expression. This balance was also recalled by the CJEU in the *Google Spain* case since the latter limits the "right to be forgotten" by a balancing with the public's right to know.

Some of these other exceptions on public health, scientific, statistical and historical interests, or defense of legal claim grounds are not surprising because they also existed in the Data Protection Directive.

ii. Council of Europe

Similarly, the Council of Europe adopted Convention 108 on January 28, 1981.[133] Convention 108 is the first binding international Treaty on personal data protection and cross-border data exchanges. It is open for the signature of non-member states of the Council of Europe. Its Article 5 provides requirements as to the quality of data.[134]

This right to erasure or deletion is implicit and underlies the data processing's purposes in Convention 108. When the purpose is reached, the data must be deleted. For instance, Russia, which is a Council of Europe member, ratified Convention 108 in 2006 and enacted the Russian Data Protection Act.[135] This Act contains similar provisions to those in the Data Protection Directive. Its Article 5(6) provides that, "[i]n the course of personal data processing it shall be necessary to ensure the personal data accuracy, their sufficiency and in case of need their adequacy for processing purposes. Operators shall take the required measures or ensure their adoption to delete or specify incomplete or inaccurate data."[136]

133. *See* Convention 108, *supra* note 105. Countries that are both member states of the Council of Europe and signatories of Convention 108 are: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Turkey, Ukraine, and the United Kingdom. A signatory of Convention 108 who is not a member state is Uruguay. In addition, non-member states, Mauritius, Morocco, and Senegal, asked for their adhesion. *See* COUNCIL OF EUROPE, CHART OF SIGNATURES AND RATIFICATIONS OF TREATY 108, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG (last visited Apr. 27, 2016) [hereinafter COE C108 SIGNATORIES].

134. Convention 108, *supra* note 105, art. 5.

135. *See* FEDERAL'NYII ZAKON OT 27 IULIA 2006 GODA N153-FZ O PERSONAL'NYKH DANNYKH [FEDERAL LAW OF 27 JULY 2006 N 152-FZ ON PERSONAL DATA], Federal'naia Sluzhba po Nadzoru v Sfere Sviazi, Informatzionnykh Tekhnologii i Massovykh Kommunikatzii [The Federal Service for Supervision of Communications, Information Technology, and Mass Media] 2006 (Russ.), http://pd.rkn.gov.ru/authority/p146/p164.

136. *See id.* art. 5(6).

iii. Non-EU European Countries

Legislation similar to the Data Protection Directive has been enacted by European countries that are not EU members. Some of them (particularly, those that are members of the EEA) have implemented the fundamental terms of the Data Protection Directive. This is the case of Norway with its Personal Data Act ("Norwegian PDA").[137] Section 27 of the Norwegian PDA on rectification of deficient personal data provides: "If personal data which are inaccurate or incomplete or of which processing is not authorized, the controller shall on his own initiative or at the request of the data subject rectify the deficient data."[138]

Some other nations' legislative acts have been recognized as providing an "adequate level of protection" in compliance with the Data Protection Directive's Article 25. In particular, this is the case in Switzerland,[139] where personal data processing is regulated by the Swiss Federal Act on Data Protection,[140] which recognizes a right to delete.[141] In a similar manner, Guernsey enacted a Data Protection Law,[142] which resembles the corresponding legislation in the United Kingdom.[143] In 2003, the European Commission found the Guernsey Law provided an adequate level of protection.[144] Its Article 14(1) provides that where it is satisfied that personal data are inaccurate a court may order a data controller "to rectify, block, erase or destroy those data and any other personal data . . . which contain an expression of opinion which appears to the court to be based on the inaccurate data."[145] Jersey's Data Protection Law came into force on December 1, 2005,[146] and the European Commission held it adequate for the purposes of the Data Protection Directive.[147] Article 14(1) of the Jersey Law is substantially similar to

137. *See* Act of Apr. 14, 2000, No. 31 relating to the processing of personal data (Nor.), https://www.datatilsynet.no/English/Regulations/Personal-Data-Act-/.

138. *Id.* § 27.

139. *See* Commission Decision 2000/518/EC, 2000 O.J. (L 215) 1.

140. *See* Bundesgesetz über den Datenschutz [DSG] [Federal Act on Data Protection] June 19, 1992, SR 235.1 (Switz.), https://www.admin.ch/opc/en/classified-compilation/19920153/201401010000/235.1.pdf.

141. *Id.* at art. 5(1).

142. *See* The Data Protection (Bailiwick of Guernsey) Law, 2001 (Guernsey), http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=71705&p=0 [hereinafter Guernsey DPL].

143. *See* Data Protection Act 1998, c. 29 (Eng.), http://www.legislation.gov.uk/ukpga/1998/29.

144. *See* Commission Decision 2003/821/EC, 2003 O.J. (L 308) 27.

145. *See* Guernsey DPL, *supra* note 142, at art. 14(1).

146. *See* Data Protection (Jersey) Law 2005, L.2/2005 (Jersey), http://www.jerseylaw.je/Law/Display.aspx?url=%2flaw%2flawsinforce%2fhtm%2fLawFiles%2f2005%2fL-02-2005.pdf [hereinafter Jersey DPL].

147. *See* Commission Decision 2008/393/EC, 2008 O.J. (L 138) 21.

Article 14(1) of the Guernsey Law.[148] The Isle of Man's legal standards on the protection of personal data are based on those of the Data Protection Directive and have been provided for in the Manx Data Protection Act.[149] In 2004, this legislation was recognized by the European Commission as providing an adequate level of protection of personal data.[150] The Faeroese Data Protection Act was found by the European Commission to cover all the basic principles necessary for an adequate level of protection.[151] Finally, Andorran legal rules for the protection of personal data are largely based on the same standards,[152] and the country has also ratified Convention 108.[153] On October 19, 2010, the European Commission recognized that Andorra had an adequate level of protection of personal data.[154]

In addition, certain other non-European countries have been recognized as having legislation providing an adequate level of data protection. For instance, the European Commission decided that the Protection of Privacy Law enacted by Israel ensures an adequate level of data protection.[155]

b. North America

i. United States

The approach of the U.S. toward privacy is inherently different from that taken by the EU, and it applies a "sector-by-sector" approach[156] that "relies on a mix of legislation, regulation, and self-regulation."[157]

Nonetheless, the first U.S. federal legislation on privacy—the Privacy Act—dates back to 1974.[158] The Privacy Act sets forth procedures for the use of "personally identifiable information" about individuals by

148. *See* Jersey DPL, *supra* note 146, at art. 14(1).

149. Data Protection Act 2002, c. 2 (Isle of Man), https://www.gov.im/lib/docs/odps/dpa2002.pdf.

150. *See* Commission Decision 2004/411/EC, 2004 O.J. (L 208) 48.

151. *See* Commission Decision 2010/146/EU, 2010 O.J. (L 58) 17.

152. Llei 15/2003, del 18 de Desembre, Qualificada de protecció de dades personals [Qualified Law 15/2003 of December 18 on the protection of personal data] (Andorra).

153. *See* COE C108 SIGNATORIES, *supra* note 133.

154. *See* Commission Decision 2010/625/EU, 2010 O.J. (L 277) 27.

155. *See* Commission Decision 2011/61/EU, 2011 O.J. (L 27) 39.

156. *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1974 (2013).

157. *U.S.-EU Safe Harbor Overview*, EXPORT.Gov, http://build.export.gov/main/safeharbor/eu/eg_main_018476 (last updated Dec. 18, 2013).

158. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)). *See United States of America*, COUNCIL OF EUROPE, http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/USA_en.asp (last visited Mar. 21, 2016).

U.S. federal agencies.[159] The Privacy Act "establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[160] The Privacy Act allows a right of access to records by their data subject,[161] and, subject to conditions, a right to request amendment;[162] however, it does not provide a right to deletion.

The Children's Online Privacy Protection Act ("COPPA")[163] is a federal law that provides certain privacy protections for children. It is aimed at any "operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child," and so does not apply to information that adults might furnish about children.[164] It is supplemented by the Children's Online Privacy Protection Rule ("COPPA Rule"), implemented by the Federal Trade Commission ("FTC"). The amendment of which became effective on July 1, 2013.[165] A "child" is defined under the COPPA Rule as "an individual under the age of 13."[166] COPPA requires an operator to obtain "verifiable parental consent"[167] before collecting, using, or

159. 5 U.S.C. § 552a (2012).

160. U.S. DEPT. OF JUSTICE, PRIVACY ACT OF 1974, http://www.justice.gov/opcl/privacy-act-1974 (last visited Mar. 21, 2016).

161. 5 U.S.C. § 552a(d)(1).

162. *Id.* § 552a(d)(2).

163. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277 tit. XIII, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501–6508 (2012)).

164. 15 U.S.C. § 6502.

165. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2015). A footnote to the supplementary information on the COPPA Rule clarifies that, "COPPA does not govern information collected by an operator offline." Children's Online Privacy Protection Rule, Final Rule Amendments, 78 Fed. Reg. 3972, 3973 n.13 (Jan. 17, 2013).

166. 16 C.F.R. § 312.2.

167. Verifiable consent is defined as:

> [M]aking any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:
>
> (1) Receives notice of the operator's personal information collection, use, and disclosure practices; and
>
> (2) Authorizes any collection, use, and/or disclosure of the personal information.

16 C.F.R. § 312.2.

disclosing "personal information"[168] from children,[169] with limited exceptions, such as where the information is collected for the child's safety and where there is a reasonable effort to provide the parents with notice, and such information is not used to contact the child, and is "not disclosed on the website or online service."[170] The website or online service operator must give parents the opportunity to refuse further use or online collection of the child's personal information, and they may direct the operator to delete their child's personal information.[171]

The COPPA Rule must be read with a broad definition of "*collects* or *collection*" in mind.[172] In addition, the COPPA Rule adds a new provision about the data retention period, and the deletion of data following such period:

> An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.[173]

This right to deletion is explicit, reserved to parents, limited to children under thirteen years old, and other limitations apply. Finally, this right to deletion is also limited to very specific circumstances, and one could argue that it actually aims to ensure that there has been adequate consent by an adult—one who is responsible for the child, which is to say his or her parent—in order to maintain data on the Internet. This is understandable, for example, given the lack of the legal capacity to contract by children.

Nevertheless, the FTC has certain powers relevant to the right to deletion, as discussed by then-FTC Commissioner Julie Brill:

> [The FTC] has authority under Section 5 of the FTC Act to prohibit "unfair" or "deceptive" practices. Because the [FTC]'s Section 5

168. "Personal information" includes names, addresses, e-mail addresses, identifiers or pseudonyms that lead to e-mail addresses, telephone numbers, Social Security numbers, persistent identifiers (such as in cookies), or certain combinations of information (such as with photographs) permitting the contacting of the child. *Id.* § 312.2. The Federal Trade Commission has also made it clear that it considers "children's photographic images, videos, and voice recordings," elements which may permit the contacting of a child, in connection with other information, as does geo-localization data, so as to include them with the definition of personal information. Children's Online Privacy Protection Rule, Final Rule Amendments, 78 Fed. Reg. at 3982.

169. 16 C.F.R. § 312.5(a)(1).

170. 16 C.F.R. § 312.5(c)(4).

171. *Id.* § 312.6(a)(2).

172. *Id.* § 312.2.

173. *Id.* § 312.10.

> authority is broad and remedial, the [FTC] has been able to require companies to allow consumers to delete or suppress information about themselves in some circumstances.
>
> For example, in our settlement with Facebook, we required Facebook to ensure that information is actually deleted or rendered inaccessible within 30 days after a consumer marks the information for deletion or terminates her account.[174]

Thanks to Section 5 of the FTC Act, the FTC is, today, the de facto privacy regulator in the U.S., although it could be argued that this role is based on consumer protection, as opposed to the fundamental rights basis for privacy and data protection in the EU.

In addition, many U.S. states have enacted laws with deletion requirements. For example, the new Rhode Island Identity Theft Protection Act provides certain requirements regarding personal information deletion, in connection with a "risk-based information security program."[175] However, there is still no omnibus legislation in the U.S. providing a right to deletion.

ii. Canada

Canadian federal legislation may be classified somewhere between the American conception of privacy and the European conception of data protection. The Personal Information Protection and Electronic Documents Act ("PIPEDA") governs how the private sector collects, uses or discloses personal information in the course of commercial business.[176] PIPEDA requires that "every organization shall comply with the obligations set out in" Schedule 1,[177] which contains principles for the protection of personal information, subject to certain exceptions. An individual is given a right to access and to correct personal data concerning him or her and Clause 4.5.3 of Schedule 1 to PIPEDA requires that "[p]ersonal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information."[178] In 2001, the European

174. Evan Selinger & Woodrow Hartzog, *Why you Have the Right to Obscurity*, CHRISTIAN SCI. MONITOR (Apr. 15, 2015), http://fw.to/6Hn8C1c. 15 U.S.C. § 45 (2012) corresponds to Section 5 of the Federal Trade Commission Act ("FTC Act") after codification.

175. Rhode Island Identity Theft Protection Act of 2015, 2015 R.I. Pub. Laws 138 (codifed at 11 R.I. GEN. LAWS § 11-49.3-2(a) (2015)).

176. Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c 5 (Can.).

177. *Id.* 5(1), at 6.

178. *Id.* 4.5.3, at 49.

Commission recognized that the Canadian PIPEDA guarantees an "adequate level of protection of personal data."[179]

c. Latin America

The Latin American view of data protection is similar to that in the EU under the Data Protection Directive. As one author stated, unlike the U.S., "[d]ata privacy legislation in Latin America, like that of the EU, involves comprehensive regulation governing the collection, use and dissemination of personal information in both the public and private spheres."[180] Latin American personal data legislation has developed in various forms and ways, and it can be divided into "two waves," with the first wave coming shortly after adoption of EU Member State legislation transposing the Data Protection Directive (Chile, Argentina, and Paraguay), followed by a second more recent wave (including Uruguay, Mexico, Costa Rica, Peru, Nicaragua, and Colombia).[181] Generally, these legislative instruments provide data subjects with rights to access, correct, amend and delete their personal data.[182]

For instance, in Argentina the Personal Data Protection Law was enacted in 2000,[183] providing data subjects with a right to correction, updating, and deletion (or a "rectification, updating or suppression right") of their personal data,[184] subject to certain exceptions.[185] Furthermore, data contained in databases must be used exclusively for the purpose for which they were legally obtained and be deleted on completion of that purpose,[186] and incomplete, or partially or totally false, data must be immediately amended or suppressed.[187] On June 30, 2003, the European Commission recognized that Argentina provides an "adequate" level of protection of personal data.[188]

In Uruguay, the Data Protection Act provides protection for personal data.[189] With this Act, Uruguay joined the short list of countries found to offer an adequate level of data protection, as determined by the European

179. *See* Commission Decision 2002/2, art. 1, 2002 O.J. (L 2/13) 15 (EC).

180. Camila Tobón, *Data Privacy Laws in Latin America: An Overview*, 44 INT'L L. NEWS, Spring 2015, at 1, 4.

181. *Id.* at 4; *see also id.* at 6.

182. *Id.* at 6.

183. *See* Law No. 25326, Oct. 4, 2000, [LX-E] A.D.L.A 5426 (partially promulgated), http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044147.pdf (Arg.).

184. *Id.* § 16, at 8.

185. *Id.* § 17, at 9.

186. *Id.* § 4(7), at 3.

187. *Id.* § 4(5), at 3.

188. *See* Commission Decision 2003/490, art. 1, 2003 O.J. (L 168) 19 (EC).

189. Ley no. 18331, Augusto, 11, 2008 [27549] Diario Oficial [D.O.] (Uru.), http://www.derecho-comercial.com/files/L18331D414uy.pdf.

Commission in line with the Data Protection Directive.[190] Articles 7 and 8 of Uruguay's Data Protection Act recognize, respectively, principles of veracity (data quality) and purpose limitation, which may lead to a right to deletion if data are not accurate or if no longer relevant or necessary for the purpose for which they were collected.[191] On April 12, 2013, Uruguay was the first non-European country to accede to Convention 108 and its Additional Protocol,[192] perhaps signaling the growing influence of the European legal instruments on data privacy issues in Latin America.

Costa Rica's data protection law was enacted in 2011 and requires explicit data subject consent for any processing of data.[193] Its Article 7(2) provides data subjects with a right of rectification, meaning the

> [R]ight to obtain, if applicable, the rectification of the personal data and their update or elimination when they were processed by violation of the provisions of this law is guaranteed, especially due to the incomplete or inexact character of the data, or because they were compiled without authorization from the data subject.[194]

Colombia's data protection law was enacted in 2012.[195] Even with the data subject's consent, the controller can process the personal data only for a limited time and consistent with the purpose for which the data was collected: Once the objectives of the processing have been fulfilled, the controller is required to suppress the personal data, unless such data must be maintained to comply with a legal, contractual or administrative obligation.[196]

The Peruvian Law for Personal Data Protection was enacted in July 2011, and its Article 20 provides the data subject a right to updating, inclusion, rectification, and deletion of his or her personal data when inaccurate, incomplete, when no longer necessary or relevant for the purpose for which they were collected, or after the time period for their

190. *See* Commission Decision 2012/484, art. 1, 2012 O.J. (L 227) 11. *See also Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited Apr. 27, 2016).

191. *See* Ley no. 18331, *supra* note 189, arts. 7–8.

192. *See* Convention 108, *supra* note 105.

193. Ley sobre la protección de la persona frente al tratamiento de sus datos personales, Ley no. 8968, Julio 7, 2011, [170] LA GACETA [D.O.] 3 (Costa Rica), http://web.ita.doc.gov/ITI/itiHome.nsf/9b2cb14bda00318585256cc40068ca69/11024d15acfca22185257a78004adfdb/$FILE/Costa%20Rica%20Data%20Protection%20Legislation%20Draft%20June%202011_EN%20translation%20by%20ITA.pdf (English trans.).

194. *Id.* art. 7(2), at 7.

195. L. 1581, Octubre 17, 2012, [48587] DIARIO OFICIAL [D.O.] (Colom.).

196. Decreto 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012, Junio 27, 2013, DIARIO OFICIAL [D.O.], art. 11 (Colom.).

processing.[197]

The Mexican Federal Personal Data Protection Law ("LFPDPPP") was published in 2010.[198] Data subjects have certain rights in connection with their personal data, such as the rights of access, rectification, deletion, or opposition, which they may exercise.[199] Pursuant to Article 24 of the LFPDPPP, a data subject has a right to a rectification or correction of his or her personal data that are inaccurate or incomplete.[200] In addition, a data subject has a right to deletion of his or her personal data,[201] subject to certain exceptions (e.g., where the data are necessary for the performance of a contract).[202] The LFPDPPP has been described as having been directly inspired by European law—both Convention 108 and the Data Protection Directive.[203]

Paraguay's Constitution recognizes the right of "habeas data,"[204] and its Personal Data Protection Law, enacted in 2000,[205] and amended in 2002,[206] regulates the collection, storage, distribution, publication, and modification of personal data contained in public or private databases.[207] Article 7 of this Law, as amended, requires that in event that certain personal data in the financial or commercial context are erroneous, inaccurate, ambiguous or incomplete, the person affected by this has the right to request and have modified, updated or deleted the data for which the request is justified.[208]

In Chile, privacy and data protection are governed by the Protection

197. Ley no. 29733, Julio 3, 2011, [11455] El peruano [D.O.] [445746], [445749] (Peru), http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc01_2011.nsf/d99575da99ebfbe305256f2e006d1cf0/e175db5cb4372b5c052578e3005321db/$FILE/NL20110703.PDF.

198. Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP] [Federal Law on Protection of Personal Information Held by Private Parties], Diario Oficial de la Federación [DOF] May 7, 2010, (Mex.).

199. *Id.* art. 22.

200. *Id.* art. 24.

201. *Id.* art. 25.

202. *Id.* art. 26.

203. *See, e.g.*, Teresa Maria Geraldes Da Cunha Lopes, *El Derecho a la Intimidad y la Protección de Datos en la Era de la Seguridad global. Principios constitucionales versus riesgos tecnológicos* [The Right to Privacy and Data Protection in the Age of Global Security. Constitutional principles versus technological risks] 48 ANUARIO JURÍDICO Y ECONÓMICO ESCURIALENSE 159, 174 (2015) ("Tanto en el espíritu como en la letra, es evidente que los legisladores mexicanos se apoyaron e inspiraron directamente en el marco normativo europeo").

204. Constitución Nacional, art. 135 (Para.), http://www.oas.org/juridico/spanish/par_res3.htm.

205. Protección de Dataos de Carácter Personal en el Paraguay, L. 1682/2001, Enero 16, 2001, http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/8F7EC36BB743626D052577C1007243CC/$FILE/Protecci%C3%B3n_d_Datos.pdf.

206. L. 1969/2002, Septiembre 3, 2002.

207. *Id.* art. 1 (amending art. 1 of L. 1682/2001).

208. *Id.* art. 1 (amending art. 7 of L. 1682/2001).

of the Private Life Act,[209] which is applicable and mandatory to every public or private entity dealing with the gathering, recording, storage and management of personal data, including employers. That Act was last amended on February 14, 2012.[210] In August 2014, Chile launched a public consultation on its preliminary draft of a data protection bill, self-described to be based on, *inter alia*, the EU Data Protection Directive, the GDPR, OECD instruments, and several Latin American data protection acts (Uruguay, Costa Rica, and Colombia).[211] According to one South American commentator, "the fact that Chile is looking not only to the EU [Data Protection] directive but also to regional laws means that there will be a trend towards harmonization in the region."[212]

Other Latin American countries are at different stages of advancement in terms of data protection legislation. For example, in Brazil, there are general principles and provisions on data protection and privacy in the 1988 Federal Constitution,[213] in the Brazilian Civil Code,[214] and in other laws (e.g., the Consumer Protection Code[215]). Furthermore, the "*Marco Civil da Internet*"[216] ("Internet Legal Framework") core rights of the Internet include freedom of access,[217] expression,[218] privacy,[219] net neutrality,[220] and data protection.[221] In this context, a right of deletion of personal data provided to certain Internet applications upon termination of a relationship between parties is provided, unless required for mandatory

209. Law No. 19628, Ley sobre protección de la vida privada, Agosto 18, 1999, DIARIO OFICIAL [D.O.] (Chile).

210. Law No. 20575, Establece el principio de finalidad en el tratamiento de datos personales, Febrero 14, 2012, DIARIO OFICIAL [D.O.] (Chile).

211. *Ante proyecto de Ley Protección de las Personas del Tratamiento de Datos Personales* [Preliminary Data Protection Bill], MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO [Ministry of Economy, Development and Tourism], http://www.participacionciudadana.economia.gob.cl/consultas-ciudadanas-virtuales/ante-proyecto-de-ley-proteccion-de-las-personas-del-tratamiento-de (last visited Apr. 8, 2016).

212. *See, e.g.*, *Chile Opens Public Consultation for Data Protection Bill*, DATA PRIVACY LAWS (July 26, 2014), http://www.dataprivacylaws.com.ar/2014/07/26/chile-opens-public-consultation-for-data-protection-bill/.

213. *See* CONSTITUIÇÃO FEDERAL [C.F.] [CONSTITUTION] art. 5(10) (Braz.).

214. *See* Lei No. 10.406 de 10 de Janeiro de 2002, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] art. 21 (Braz.).

215. *See generally* Lei 8.078 de 11 de Setembro de 1990, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] 12.09.1990 (Braz.).

216. Lei No. 12.965 de 23 de Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.04.2014 (Braz.) [hereinafter Lei No. 12.965]. For a discussion of the Internet Legal Framework see Renato Opice Blum, Rony Vainzof, & Rita P. Ferreira Blum, *Know More About the Brazilian "Internet Legal Framework"*, 70 BUS. LAW. 313 (2014).

217. Lei No. 12.965 *supra* note 216, art. 4.

218. *Id.* arts. 2, 3(I).

219. *Id.* arts. 3(II), 7.

220. *See id.* arts. 3 (IV), 9.

221. *See id.* arts. 3 (III), 7.

recordkeeping under law.[222] A new version of a Draft Data Protection Act, which would recognize some principles similar to those of the EU Data Protection Directive, was presented by the Brazilian Ministry of Justice in October 2015.[223] The Draft Data Protection Act provides for data subject rights including rights of access and deletion of personal data.[224]

Venezuela's Constitution guarantees privacy.[225] In addition, it provides for certain data subject rights with respect to their data such as a right to deletion in certain circumstances, such as when erroneous or when their rights are unlawfully affected. The enforcement of these data subject rights may be sought by petition to a competent court.[226]

d. South Pacific

Australian privacy and data protection exists both at the Federal and at the State/Territory levels. The Federal Privacy Act of 1988, as amended and its new Australian Privacy Principles ("APPs") apply to private sector entities, which are generally included within the definition of the term "organization," which is itself a component of the term "APP entity."[227] The Privacy Act was amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012,[228] bringing it closer to the EU data protection regime. APP Principle 13.1 requires correction of personal information by an agency or organization (an "APP entity") if satisfied that "the information is inaccurate, out-of-date, incomplete, irrelevant or misleading," or if rightfully requested by the individual to do so.[229] In

222. *See id.* art. 7 (X).

223. Press Release, Ministry of Justice, MJ apresenta nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais [MoJ presents new version of the Draft Personal Data Protection Law] (Oct. 20, 2015) (Braz.), http://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais.

224. *See* Anteprojeto de Lei, Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural [Draft Legislation on the Regulation and Treatment of Personal Data to Guarantee Freedom and Dignity of Personality Development of Natural Persons], art. 18, http://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf.

225. Constitución de la República Bolivariana de Venezuela [Constitution of the Bolivarian Republic of Venezuela], GACETA OFICIAL [OFFICIAL GAZETTE], Diciembre 30, 1999, No. 36860, art. 60.

226. *Id.* art. 28.

227. *See Privacy Act 1988* (Cth) pt 2, s 6(1) (Austl.). As private sector entities are generally organizations (as that term is defined, by cross-reference to *id.* s 6C; although see the exclusion from this term of certain "small business operators"), and thus fit within the definition of an "APP entity," they are required not to breach APPs: "An APP entity must not do an act, or engage in a practice, that breaches an Australian Privacy Principle." *Id.* s 15.

228. *See* Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) (Austl.). The amendments introduced new powers for the Privacy Commissioner, and introduced the APPs. For a short discussion of the Privacy Amendment Bill 2012, see W. Gregory Voss et al., *Privacy, E-Commerce, and Data Security*, 47 ABA/SIL YIR 99, 111 (2013).

229. *Privacy Act 1988*, *supra* note 227, sched. 1, princ. 13.1 (Austl.).

addition, where the personal information is no longer necessary and where its retention is not mandated by law, the APP entity may be required to take reasonable steps to "to destroy the information or to ensure that the information is de-identified."[230]

New Zealand's Privacy Act (1993)[231] establishes how "agencies" (which may be in the public or private sector) collect and use personal information, and provides in its Principle 7 an obligation and a right to correction.[232] On December 19, 2012, the European Commission decided, pursuant to the Data Protection Directive, that New Zealand law provides an adequate level of data protection.[233]

e. Asia

Japan figures among the early adopters of omnibus data protection legislation in Asia. The Japanese Act on the Protection of Personal Information ("APPI") came into force on April 1, 2005.[234] APPI's Article 26(1) provides an individual with a right to request correction, addition, or deletion of personal data, where the current data is inaccurate ("contrary to the fact").[235] In addition, Article 27(1) provides that where personal information has been improperly obtained or is being used for an illegitimate purpose, an individual may have a right to request erasure in certain circumstances.[236]

India's Ministry of Communications and Information Technology adopted the "Privacy Rules" in 2011.[237] Rule 5(6) of these Privacy Rules requires that a

> [b]ody corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.[238]

Nonetheless, the Privacy Rules do not contain a specific right to require

230. *Id.* sched. 1, princ. 11.2 (Austl.).

231. *See* Privacy Act 1993 (N.Z.).

232. *Id.* s 6, princ. 7.

233. *See* Commission Decision 2013/65/EU, 2013 O.J. (L 28) 12.

234. Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information], Act No. 57 of 2003, translated in (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/ (Japan).

235. *Id.* art. 26, ¶ 1.

236. *Id.* art. 27, ¶ 1.

237. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011) (India).

238. *Id.* r. 5(6).

deletion, erasure, or destruction of personal information or data.

Since 2010, additional Asian countries have enacted data protection legislation. The Personal Data Protection Act was passed by the Malaysian Parliament on June 2, 2010.[239] Its Section 10(2) requires that: "It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed."[240] In addition to this right under the retention principle, other data protection principles are set out in the Act, such as data integrity and access principles.[241]

In South Korea, a Personal Information Protection Act ("PIPA") was enacted and became effective as of September 30, 2011, and has subsequently been amended, most recently in 2014.[242] PIPA's Article 21(1) requires:

> When personal information becomes unnecessary as its holding period expires, its management purpose is achieved and by any other ground, a personal information manager shall destroy the personal information without delay: *Provided*, That this shall not apply where the personal information must be preserved pursuant to any other statute.[243]

Requests for deletion of unnecessary data are allowed, subject to legal requirements, and in this sense, commentators have noted that, "Korea does have something close to the 'right to be forgotten.'"[244]

In Hong Kong, the Personal Data (Privacy) Ordinance provides the legal framework for data protection.[245] The Ordinance was substantially modified by the Personal Data (Privacy) (Amendment) Ordinance in 2012.[246] As amended, the Ordinance provides for erasure of personal data no longer required for "the purpose (including any directly related purpose) for which the data was used," unless prohibited by law or where erasure is not in the public interest (e.g., for historical reasons).[247]

Singapore enacted the Personal Data Protection Act in 2012.[248] Its

239. Personal Data Protection Act 2010, Act No. 709, (Royal Assent, June 2, 2010; Publication in the Gazette, June 10, 2010) (Malay.).

240. *Id.* § 10(2).

241. *Id.* §§ 11–12.

242. Gae-in Jeong-bo Bo-ho Bop [Personal Information Protection Act] (S. Kor.), http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32442&lang=ENG.

243. *Id.* art. 21(1).

244. Graham Greenleaf & Whon-il Park, *South Korea's Innovations in Data Privacy Principles: Asian Comparisons*, 30 COMPUTER L. & SECURITY REV. 492, 503 (2014). For additional discussion of Korean developments, see Voss et al., *supra* note 228, at 112–113.

245. Personal Data (Privacy) Ordinance, (2013) Cap. 486, (H.K.).

246. Personal Data (Privacy) (Amendment) Ordinance 2012, No. 18, (2012) O.H.K. (H.K.).

247. Personal Data (Privacy) Ordinance, *supra* note 245, § 26(1), as amended by Personal Data (Privacy) (Amendment) Ordinance 2012, *supra* note 246, § 17.

248. Personal Data Protection Act 2012, No. 26 of 2012 (Sing.).

Article 22(1) provides that "[a]n individual may request an organization to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organization."[249] Where no longer necessary for the original purpose for which collected or for retention for legal or business purposes, documents containing personal data shall no longer be retained, or the organization shall "remove the means by which the personal data can be associated with particular individuals."[250]

Currently in China there is not an omnibus data protection law, but data protection may be found in various laws and regulations. Specially, China amended its Law on the Protection of Consumer Rights and Interests (the "New Consumer Law").[251] The New Consumer Law applies to all types of business that deals with consumers and provides greater rights to consumers, including the explicit recognition of consumers' rights to their personal data,[252] in addition to the introduction of data privacy principles.[253]

f. Africa

Many African nations have enacted omnibus data protection legislation providing a right to deletion or, at a minimum, a right to correction. Burkina Faso enacted Act No. 010-2004 in 2004,[254] and it provides a right to correction.[255] The Tunisian Data Protection Act requires erasure (or destruction) of data at the end of the specified or authorized retention period (or of such period mandated by specific laws), [256] or when their purpose for collection has been achieved or where no longer necessary for the activity of the data controller.[257] In addition, the right to

249. *Id.* § 22(1).

250. *Id.* § 25.

251. Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Xiugai «Zhonghua Renmin Gongheguo Xiaofei Zhe Quanyi Baohù Fa» de Jueding 全国人大常委会关于修改《中华人民共和国消费者权益保护法》的决定 (2013) [现行有效] [Amending the Law of the People's Republic of China on the Protection of Consumer Rights and Interests] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 25, 2013, effective Mar. 14, 2014) (Lawinfochina) (China).

252. *Id.* art. 14.

253. *Id.* art. 29.

254. Loi No. 010-2004/AN Portant Protection des Données à Caractère Personnel [Act no. 010-2004/AN on the Protection of Personal Data] (Apr. 20, 2004) (Burk. Faso), http://www.afapdp.org/wp-content/uploads/2012/01/Burkina-Faso-Loi-portant-protection-des-données-à-caractère-personnel-20042.pdf.

255. *Id.* art. 17.

256. Loi organique No. 2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel [Organic Act No. 2004-63 of July 27, 2004 on the Protection of Personal Data] (Tunis.) (French version), http://www.e-justice.tn/fileadmin/fichiers_site_francais/droits_homme/legis_nat/lib_pub/L_2004_63.pdf.

257. *Id.* art. 45.

deletion, in case of data being inaccurate, ambiguous, or where their processing is unlawful, exists within the concept of right of access.[258]

In Mauritius, the Data Protection Act No. 13/2004 recognized a right to deletion of inaccurate personal data[259]: "A data controller shall, upon being informed as to the inaccurateness of personal data, by a data subject to whom such data pertains, cause such data to be rectified, blocked, erased or destroyed, as appropriate."[260] Where the data controller fails to do so, the data subject may apply to the Data Protection Commissioner for the same relief.[261] This right is in addition to the duty for a data controller to destroy data, "[w]here the purpose for keeping personal data has lapsed."[262]

Under the Senegalese Data Protection Act,[263] inaccurate or incomplete data must be deleted or corrected.[264] Morocco's Data Protection Act[265] provides that inaccurate or incomplete data be corrected or erased.[266] In addition, a specific right is granted to the data subject to obtain from the data controller the correction, updating, deletion or blocking of data whose processing is not in compliance with the Act, notably because the data is incomplete or inexact, within ten days, without charge to the data subject.[267] In Benin, an individual may request that his or her "erroneous, incomplete, equivocal, expired personally identifiable information; or of which the collecting, the usage, the communication or the storage are forbidden; be rectified, completed, updated, secured or deleted."[268] Similarly, the Gabon Data Protection Act[269] provides data

258. *Id.* art. 32.

259. The Data Protection Act 2004, Act 13/2004, June 17, 2004, as amended (Mauritius), http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Data%20Protection%20Act%202004_Maurice.pdf.

260. *Id.* art. 44(1).

261. *Id.* art. 44(4).

262. *Id.* art. 28(1).

263. Loi no. 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel [Law No. 2008-12 on personal data Protection] (in French) (Sen.), http://www.cdp.sn/images/doc/protection.pdf.

264. *Id.* art. 36.

265. Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel [Law No. 09-08 on the protection of individuals with regard to the processing of personal data], Feb. 18, 2009 (Morocco), http://www.cndp-maroc.org/images/lois/Loi-09-08-Fr.pdf.

266. *Id.* art. 3(1)(d).

267. *Id.* art. 8(a).

268. Loi n° 2009-09 portant protection des données à caractère personnel en République du Bénin [Law No. 2009-09 of May 22, 2009 on dealing with the protection of personally identifiable information (PII) in the Republic of Benin] May 22, 2009, art. 15 (English translation), http://www.cnilbenin.bj/images/Texte/Loi%20No%202009%20du%2022Mai%202009%20Version%20Anglaise.pdf.

269. Loi n°001/2011 relative à la protection des données à caractère personnel [Act No.

subjects with a right to deletion.[270]

The Angolan Data Protection Act ("Angolan DPA") was enacted in June 2011.[271] The Angolan DPA was inspired by the EU Data Protection Directive,[272] and its Article 28 provides a right to deletion if data are incomplete or inaccurate.[273] Ghana's Data Protection Act[274] provides data subjects with a right to deletion when data is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully,"[275] as well as a right to deletion of destruction of data held beyond the authorized retention period.[276] Cape Verde's Data Protection Act provides a right to deletion or rectification of inaccurate or incomplete data.[277] Many underlying similarities between the Cape Verdean Act and the Data Protection Directive are "due to the fact that, while drafting the Act, the Cape Verdean legislator chose to borrow heavily from the Portuguese Data Protection Law" that implemented the Data Protection Directive.[278]

Finally, South Africa's Protection of Personal Information Act ("PPI Act")[279] provides that a data subject may request deletion or correction of personal information that is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully," or request destruction or deletion of personal information that the responsible party is no longer authorized to retain under Section 14 of the PPI Act.[280]

001/2011 on Personal Data Protection], JOURNAL OFFICIEL DE LA REPUBLIQUE GABONAISE [OFFICIAL GAZETTE OF GABON], No. 74, Oct. 24-31, 2011), p. 491 (Gabon), http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-à-la-protection-des-données-personnelles-du-4-mai-20112.pdf.

270. *Id.* art. 14, at 493.

271. Lei No. 22/11, de 17 de Junho de 2011—Da Protecção de Dados Pessoais [Act No. 22/11 of June 17, 2011—Data Protection [hereinafter Angolan DPA)] (Angola).

272. "The framework laid down by the [Angolan] DPA is strongly inspired by, and follows the same basic principles as, the EU Data Protection Directive." W. Gregory Voss et al., *Privacy, E-Commerce, and Data Security*, 46 INT'L LAWYER 97, 108 (2012).

273. Angolan DPA, *supra* note 271, art. 28.

274. Data Protection Act, 2012 Act No. 843 (Ghana), http://media.mofo.com/files/PrivacyLibrary/3981/GHANAbill.pdf.

275. *Id.* art. 33(1)(a).

276. *Id.* art. 33(1)(b).

277. Regime Jurídico Geral De Protecção de Dados Pessoais a Pessoas Singulares [General Legal Regime of Personal Data Protection to Individuals], Lei n°133/V/2001, de 22 de Janeiro de 2001 [Act No. 133/V/2001, of Jan. 22, 2001], BOLETIM OFICIAL [B.O.] [OFFICIAL GAZETTE OF CAPE VERDE], art. 6 (1)(d) (on data quality principle), and art. 12(1)(d) (on right to access), http://www.afapdp.org/wp-content/uploads/2012/01/Cap-vert-Lei-n°133-V-2001-do-22-janeiro-2001.pdf. Since 2014, the Cape Verdean Data Protection Agency has the power to order the erasure of data. *See* Voss et al., *Privacy, E-Commerce, and Data Security*, 48 ABA/SIL YIR 103, 117 (2014).

278. *See* João Luis Traça & Bernardo Embry, *An Overview of the Legal Regime for Data Protection in Cape Verde*, 1 INT'L DATA PRIVACY L. 249, 251 (2011).

279. Protection of Personal Information Act 4 of 2013, GN R. 912 of GG 37067 (26 Nov. 2013) (S. Afr.), https://www.issafrica.org/uploads/SA-POPI-Act-2013.pdf.

280. *Id.* § 24(1).

In addition to the above, it should be noted that Mauritius, Morocco, Senegal, and Tunisia, all non-Council of Europe states in Africa, have requested their adhesion to the Council of Europe's Convention 108.[281] Among safeguards for data subjects, Article 8 of Convention 108 provides that: "Any person shall be enabled: . . . (c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention."[282] Article 5 of Convention 108 provides protection of quality of data, including accuracy, relevance, proportionality, adequacy, etc.;[283] and Article 6 provides that special categories of data (or sensitive data) may not be processed automatically.[284] Thus an eventual adhesion of these African countries would involve their corresponding commitments on the right to deletion or erasure of data.

In summary, this article has shown that many national data protection acts were recently promulgated in Africa, Asia, and Latin America. These legal instruments confirm the influence of the EU Data Protection Directive model. The right to deletion is common in many countries and, it may be argued, reflects the influence of the Data Protection Directive. However, as this paper will show, since 2012 the "right to be forgotten" has taken on new forms in a digital context. The question today is whether this relatively new right, especially in the form this paper has identified as the "right to delisting," will be implemented in other legislation or jurisdictions beyond the EU. More generally, one may wonder how the social demand for the protection of privacy in the digital context can be met, particularly in social networks. Should a right to digital oblivion be provided for and recognized worldwide?

B. The "Right to Be Forgotten": Digital Context

In a digital context, the "right to be forgotten" takes several forms, which this paper has identified as (1) the right to delisting, and (2) the right to obscurity and the right to digital oblivion, which are ongoing.

281. *See* Council of Eur. Treaty Off., *Chart of signatures and ratifications of Treaty 108*, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=IYsGshqz (last visited May 4, 2016).

282. *See* Convention 108, *supra* note 105, art. 8.

283. *Id.* art. 5.

284. *Id.* art. 6.

1. *Right to Delisting*/Delinking/De-indexing

The right to delisting is sometimes referred to, alternatively, as the "right to delinking" or the "right to de-indexing." This right is probably the most visible of the forms of the "right to be forgotten" in the digital context, especially since the rendering of the *Google Spain* decision.

a. The Google Spain *Case*

As this paper has shown,[285] a form of the "right to be forgotten" was applied in the CJEU's *Google Spain* decision,[286] which recognized a right to delisting the results proposed by Google's search engine in certain circumstances. The ruling concerns the interpretation of Articles 2(b) and (d), 4(1)(a) and (c), 12(b) and (a), 14(a) of the Data Protection Directive, and of Article 8 of the Charter. The ruling request had been made in proceedings between, on the one hand, Google Spain and Google Inc., and on the other hand, the *Agencia Española de Protección de Datos* (Spanish Data Protection Agency; "AEPD") and Costeja. The ruling request concerned a decision by the AEPD upholding the complaint lodged by Costeja against those two companies and ordering Google Inc. to adopt measures necessary to withdraw personal data relating to Costeja from its index and to prevent access to the data in the future.

The CJEU decided that Google Inc. had to remove links to a third party's web pages from the results displayed following a search using Costeja's name, even where the name or information is not erased from such pages.[287] Moreover, in light of the data subject's fundamental rights under Articles 7 and 8 of the Charter in this case, such rights should override the operator's economic interest and the general public's interest in accessing the information using a nominative search. Nonetheless, the opposite might be the result if the data subject was to be a person with a prominent role in "public life."[288] Providing criteria for delisting, the CJEU considered that a right to delisting applied, "because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine . . . ."[289] Thus, an analysis must be made, and a balancing

285. *See supra* Introduction, section A.1.

286. *See* Case C-131/12 Judgment of the Court (Grand Chamber), Google Spain SL v. Agencia Española de Protección de Datos, CURIA paras. 89–99 (May 13, 2014) (ECLI:EU:C:2014:317), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131.

287. *Id.* at para. 88.

288. *Id.* at para. 97.

289. *Id.* at para. 94.

test applied, on a case-by-case basis.[290]

First, it must be noted that the decision involves a mere right to delisting (and not to be completely forgotten) because the court orders the erasure of a web link, but not the related article. The source is preserved. In other words, "Google can't forget you, but it should make you hard to find."[291] Next, the right to delisting may be exercised directly by contacting the search engine (without having to contact the publisher of the original source first), as data protection law applies to the activity of a search engine acting as a controller.[292]

Secondly, this ruling was surprising because it went against the opinion of the Advocate General delivered nearly one year beforehand.[293] In that opinion, the data subject was found not to have a right to go directly to the search engine service provider to request delisting.[294]

Thus, the CJEU appears to have been audacious because its interpretation of Data Protection Directive Article 12 on the right of access was very broad. Generally speaking, the right to delete provided under that Article is only required in the exercise of the right to access and in specific circumstances when data are incorrect. In *Google Spain*, the right to delisting is exercised independently of the right to access, and even if the data are correct and lawful. The erasure of negative personal information is only justified by the protection of the data subject's reputation. The circumstances to be taken into account in the balancing test go beyond the text of the Data Protection Directive. Moreover, absence of harm or prejudice to the data subject is not dispositive.

Thirdly, in order to recognize a right to delisting, neither the economic interest of the operator of the search engine nor the interest of the general public in having access to that information controls. This establishes a hierarchy in which the data subject's reputation and privacy are more important than the freedom to undertake or the freedom of expression in general. Nevertheless, the situation may be reversed if the data subject is a public figure. This contrasts strikingly with U.S. law and the importance it attributes to the freedom of expression. But in the EU,

290. For further analysis of the implementation challenges associated with the *Google Spain* decision, see Aleksandra Kuczerawy & Jef Ausloos, *From Notice-and-Takedown to Notice-and-Delist: Implementing* Google Spain, 14 COLO. TECH. L.J. 219 (2016).

291. Evan Selinger & Woodrow Hartzog, *Google Can't Forget You, but It Should Make You Hard to Find*, WIRED (May 20, 2014, 3:33 PM), http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find.

292. *See* Art. 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez" at 6, (Nov. 26, 2014).

293. Case C-131/12 Opinion of Advocate Gen. Jääskinen, Google Spain SL v. Agencia Española de Protección de Datos, CURIA para. 20 (June 25, 2013) (ECLI:EU:C:2013:424), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CC0131.

294. *Id.* at para. 138(3).

the rights to privacy and to personal data protection are fundamental rights enshrined in the Charter. Yet, freedoms of expression and information are also protected in the Charter. In the end, a balancing of interests is required.

b. The Manni *Case*

However, the *Google Spain* case did not resolve everything. In July 2015, the Italian Supreme Court asked the CJEU for a preliminary ruling[295]—which has yet to be issued—on questions regarding the "right to be forgotten."[296] The business of Salvatore Manni went bankrupt in 1992, and this fact was included on the relevant company's register, managed by defendant, allegedly causing plaintiff damages.[297] The latter requested defendant to render his name anonymous or restrict access to the register.[298]

"The Italian Court essentially wonders whether information legally consigned to (and made public by by) the defendant, can be erased, anonymised or access-restricted after a certain time."[299] Also at stake is the question of whether Article 6(1)(e) of the Data Protection Directive supersedes European and national company law requirements regarding notice on the companies register.

In this case, the CJEU is asked to assess the obligations of the original publisher of the information, unlike in *Google Spain*. In addition, in the *Manni* case, the original source of the information is required by law to publish such information. Furthermore, the CJEU is only asked whether the source can be required to make data "less accessible," not whether the data must be removed entirely.[300] It seems like a right to obscurity.

295. Case C-398/15, Manni, 2015 O.J. (C 354) 20, http://curia.europa.eu/juris/fiche.jsf?id=C;398;15;RP;1;P;1;C2015/0398/P. This involves a request for a preliminary ruling from the Italian Corte suprema di cassazione, Prima Sezione Civile (court of last appeal on issues of law in civil matters), lodged on July 23, 2015, and related to the *Manni* matter.

296. *See* Jef Ausloos, *CJEU is Asked to Rule on the 'Right to be Forgotten' Again*, TECH, POLICY, & SOC'Y (Sept. 18, 2015), https://jefausloos.wordpress.com/2015/09/18/cjeu-is-asked-to-rule-on-the-right-to-be-forgotten-again.

297. *Id.*

298. *Id.*

299. *Id.*

300. *Id.*

c. *Legislation and Case Law on the Right to Delisting Around the World*

The *Google Spain* case was widely commented on around the world.[301] Thus, one may wonder what influence this ruling will have in other countries. The right to delisting's impact on freedom of speech may be anathema for many Americans. But other countries may have a similar legal culture to that of Europeans, and the will to recognize the right to delisting, as well.

i. Legislation on the *Right to Delisting*

The current reform of the Council of Europe's Convention 108[302] in parallel with the recent reforms to the Data Protection Directive will bring new rules adapted to the evolutionary environment of data processing, but this reform neither changes data subject rights nor creates a "right to be forgotten" nor a right to delisting. This text confirms the implicit right to deletion tied to the purposes of the processing,[303] which is considered as being sufficient.[304] Nonetheless, a "right to be forgotten" in the specific context of social networks was recognized by a recommendation.[305] In addition, the Council of Europe issued another Recommendation on the protection of human rights with regard to search engines.[306] The balance of interests was already done because Member States should ensure that

301. *See* sources cited, *supra* notes 23 and 24; Jerome Squires, Case Note, Google Spain SL v Agencia Española de Protección de Datos (European Court of Justice, C-131/12, 13 May 2014), 35 ADEL. L. REV. 463 (2014) (Austl.).

302. *See* Consult. Comm. of the Convention for the Protect. of Individuals with Regard to Automatic Processing of Pers. Data, *Propositions of Modernisation of Convention* 108, Dec. 18, 2012, http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_E_Convention%20108%20modernised%20version.pdf.

303. CÉCILE DE TERWANGNE, *La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* [*Revision of the Council of Europe's Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data*], *in* QUELLE PROTECTION DES DONNEES PERSONNELLES EN EUROPE? [WHAT PROTECTION OF PRIVACY IN EUROPE?], (Céline Castets-Renard ed., 2015) (Fr.), at 81, 103.

304. *See La Commission LIBE en faveur de la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* [*The LIBE Commission in Favor of the Modernization of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data*], (Fr.), EU LOGOS ATHENA (Nov. 25, 2014), http://europe-liberte-securite-justice.org/2014/11/25/la-commission-libe-en-faveur-de-la-modernisation-de-la-convention-108-pour-la-protection-des-personnes-a-legard-du-traitement-automatise-des-donnees-a-caractere-personnel.

305. Comm. of Ministers of the Council of Eur., Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, Apr. 4, 2012 [hereinafter Recommendation CM/Rec(2012)4].

306. Comm. of Ministers of the Council of Eur., Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, Apr. 4, 2012.

any law, policy or individual request on de-indexing or filtering is enacted with full respect for relevant legal provisions, the right to freedom of expression, and the right to seek, receive, and impart information. The principles of due process and access to independent and accountable redress mechanisms should also be respected in this context. In addition, Member States should work with search engine providers so that they ensure that any necessary filtering or blocking is transparent to the user.[307]

Moreover, a new Russian law on implementation of the "right to be forgotten" was approved on July 14, 2015: the "Delisting Law," which gives individuals the right to be delisted from search engines, was slated to come into force on January 1, 2016.[308] New obligations are placed on Internet search engines, providing individual data subjects with a right to delisting. The "right to delisting" applies to information where their publication does not comply with legal requirements, as well as where the data are inaccurate or obsolete.[309]

According to one commentator, these changes to Russia's "right to be forgotten" are "making it significantly stricter than its European counterpart."[310] Two areas where the Russians are going further are that under the right, the data subject would not need to provide the URLs of information that he or she wants delisted, merely the information they seek to have deleted. In addition, the delisting right would also apply to public figures and to information where there is a public interest to know. Criticism of the "right to delisting" law came notably from Yandex, Russia's biggest search engine, which claimed that the law violates a constitutional right of access to information, according to another source.[311]

Israel already benefits from a European Commission decision that its data protection level is adequate for cross-border transfers of personal data

307. *Id.*

308. Federal'nyi Zakon o vnesenii izmenii v Federal'nyi zakon "Ob informatzii, informatzionnyx texnologiax i o zaschite informatzii" i stat'i 29 i 402 Grazhdanskogo protzessual'nogo kodeksa Rossiiskoi Federatzii [Law of the Russian Federation Amending the Federal Law "on Information, Information Technologies and Information Protection" and Articles 29 and 402 of the Civil Procedure Code of the Russian Federation], ROSSIISKAIA GAZETA [ROS. GAZ.] July 16, 2015, http://rg.ru/2015/07/16/informacia-dok.html [hereinafter Russian Delisting Law]. *See also* Irina Anyukhina, *'Right to Be Forgotten' in Russian Data Protection Law Has Passed All Stages of Approval*, NAT'L L. REV. (July 21, 2015), http://www.natlawreview.com/article/right-to-be-forgotten-russian-data-protection-law-has-passed-all-stages-approval.

309. Anyukhina, *supra* note 308.

310. Olga Razumovskaya, *Russia Proposes Strict Online Right to be Forgotten*, WALL ST. J. DIGITS (June 17, 2015, 7:09 AM), http://on.wsj.com/1JXzoHh.

311. Tetyana Lokot, *President Putin Signs Russian 'Right to Be Forgotten' Into Law*, GLOBALVOICES (July 18, 2015, 5:59 PM), https://globalvoicesonline.org/2015/07/18/president-putin-signs-russian-right-to-be-forgotten-into-law/#.

processed through automated means.[312] Section 14(a) of the Israeli Protection of Privacy Act provides a right to deletion for inaccurate or incomplete information.[313] According to one commentator, "[a] bill sponsored by a bi-partisan group of seven Knesset (Israeli Parliament) members proposes to establish persons' state of oblivion by amending the Protection of Privacy Act (PPA)."[314] This bill would allow a specific right to request deletion of information by search engines in case of violation of an individual's privacy or harm caused by publication of personal information, and a balancing test would be applied with respect to the public's right to access information.[315] Thus, this bill appears to follow the same approach presented by the CJEU in *Google Spain*.

In 2014, the Australian Law Reform Commission (ALRC)[316] proposed the introduction of a new principle into the Privacy Act that would "require an APP entity to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual."[317] An "APP entity" may refer to some private sector entities, as well as to most governmental ones.[318] Unlike the GDPR, the Australian principle would not apply to private information posted by other individuals or organizations. Thus, this right would be much more limited than in the EU.

Finally, a Brazilian legislative bill related to the right to delisting was introduced in 2014.[319] The bill has one substantive article, providing that a search engine be required to remove links that refer to any irrelevant or outdated data, upon the request of any citizen or person involved.[320]

312. Commission Decision 2011/61/EU of 31 January 2011, 2011 O.J. (L 27) 39 (Feb. 1, 2011).

313. *See* Protection of Privacy Law, 5741-1981, art. 14(a), 35 LSI 136 (1980-81) (as amended) (Isr.), *translated in Israel, Protection of Privacy Law, 5741-1981*, WORLD INTELL. PROP. ORG. (2014), http://www.wipo.int/wipolex/en/text.jsp?file_id=347462; *see also*, Art. 29 Data Prot. Working Party, Opinion 6/2009 on the level of protection of personal data in Israel, at 7 (Dec. 1, 2009) (WP 165), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf.

314. Dan Or-Hof, *The Right to be Forgotten is Headed for the Israeli Law*, LINKEDIN PULSE (July 24, 2014), https://www.linkedin.com/pulse/20140724130802-1470684-the-right-to-be-forgotten-is-headed-for-the-israeli-law.

315. *Id.*

316. AUSTL. L. REFORM COMM'N, SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA (Mar. 2014) (ALRC Discussion Paper 80) (Austl.), http://www.alrc.gov.au/sites/default/files/pdfs/publications/whole_dp80.pdf.

317. *Id.* at 15 (Proposal 15-2 (a)).

318. *See Privacy Act*, OFFICE OF THE AUSTL. INFO. COMM'R, https://www.oaic.gov.au/privacy-law/privacy-act/ (last visited Mar. 21, 2016).

319. Projeto de Lei No 7881/2014 [Bill no. 7881/2014], Nov. 11, 2014, http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=621575 (Braz.).

320. *Id.* art. 1.

ii. Case Law on the *Right to Delisting*

In September 2014, the Kyoto District Court is reported to have rejected a suit filed against Google's Japan subsidiary by a man who wanted to have his arrest record removed from its search results. According to a news article: "The judges said the case lacked legal grounds and sided with Google Japan's position that it is the U.S. parent company, not the Japanese unit, that is responsible for managing searches and therefore it is not obliged to supervise them."[321] By contrast, the Tokyo District Court in October 2014 was reported to have ordered Google to "remove the titles and snippets to websites revealing the name of a man who claimed his privacy rights were violated due to articles hinting at past criminal activity."[322] Commenting on the same case, Chuo University in Tokyo Professor Hiroshi Miyashita was reported to have said that the ruling did not set a "formal precedent" but was a "landmark for online privacy," adding, that he had "no hesitation to say that the right to be forgotten has arrived in Japan."[323] In the same vein, on June 25, 2015, the Saitama District Court in Japan ordered Google to remove from its search results details of an arrest three years earlier for child prostitution law violations, and reportedly commented that the crime was "relatively minor and has no historic or social significance."[324] Interestingly, in the latter two cases, the right to delisting is tied to the right to rehabilitation. However, with respect to privacy rights, which according to Senshu University Professor of Media Law and Journalism Kenta Yamada are "established through court precedents" and not by statute, it is reported that "Japanese judges have yet to reach a consensus on how to balance the right to privacy and the freedom of expression and of information."[325]

In Canada, the Court of Appeal for British Columbia recognized a type of "right to be forgotten" in the *Equustek Solutions Inc. v. Jack* case.[326] In that litigation, the Court confirmed an injunction requiring Google to delist (to "cease indexing" or referencing in search results) certain web sites involved in trade secrets and intellectual property

321. Tomoko Otake, *'Right to be Forgotten' on the Internet Gains Traction in Japan*, JAPAN TIMES (Dec. 9, 2014), http://www.japantimes.co.jp/news/2014/12/09/national/crime-legal/right-to-be-forgotten-on-the-internet-gains-traction-in-japan/.

322. *Id.*

323. Simon Mundy, *Asia Considers 'Right to be Forgotten' Ruling Prompted by Google*, FIN. TIMES (Mar. 12, 2015, 3:46 AM), http://www.ft.com/intl/cms/s/0/ade889d4-bc0e-11e4-a6d7-00144feab7de.html#axzz3mrfZ8F3j.

324. Kyodo, *Japan Court Orders Google to Remove Past Arrest Reports*, JAPAN TIMES (July 2, 2015), http://www.japantimes.co.jp/news/2015/07/02/national/crime-legal/japan-court-orders-google-to-remove-past-arrest-reports/#.VgbCz0slLzA.

325. Otake, *supra* note 321.

326. Equustek Solutions Inc. v. Jack, 2015 BCCA 265, June 26, 2015 (Can. B.C. C.A.), http://www.canlii.org/en/bc/bcca/doc/2015/2015bcca265/2015bcca265.html.

disputes.[327] The Court found that Google falls under the jurisdiction of British Columbia's courts because of its information-gathering (through web crawling) and advertising activities in that province.[328] On one hand, this ruling, which calls for delisting beyond the Canadian domain name ".ca"[329] is similar to that of the French data protection authority (CNIL), which required Google to apply the delisting decision to all of Google's domain names, for a global right to delisting.[330] But, on the other hand, this ruling is very different from *Google Spain*, because the plaintiff is not a natural person but a company. Moreover, the ruling is rendered with respect to an intellectual property dispute and not for questions of privacy or personal data law benefitting natural persons. Thus, this ruling involves e-reputation, but not private life. By contrast, in the *Niemela v. Malamas* case,[331] the Supreme Court of British Columbia "refused to force Google to block defamatory comments about a Vancouver lawyer, Glenn Niemela, from its global search results."[332] It "found that Google was not a 'publisher' of the defamatory material, but a 'passive instrument' and a mere 'facilitator' of the search results."[333] The right to delisting was refused. The Court's reasoning was established based on media law, regardless of privacy aspects. Thus, Canadian law cannot be considered as having recognized a clear "right to be forgotten." *Equustek Solutions Inc.* must then be seen as an isolated judgment rendered by a court of appeals for a province and not a provincial supreme court or federal court decision.

In 2015, the Colombian Supreme Court rendered a ruling on the "right to be forgotten" on a request for delisting in connection with a criminal sentence.[334] Although the Court rejected the request, it imposed an obligation to remove the first and last names of parties and witnesses from decisions that can be accessed through the databases of the Criminal Chamber of the Supreme Court.[335] Thus, in this case and as in Japan, the

327. *Id.* para. 26.

328. *Id.* para. 54.

329. *Id.* para. 107. "The plaintiffs have established, in my view, that an order limited to the google.ca search site would not be effective. I am satisfied that there was a basis, here, for giving the injunction worldwide effect."

330. Commission national de l'informatique et des libertés, Décision n° 2015-047 du 21 mai 2015 mettant en demeure la société GOOGLE INC. [Decision No. 2015-047 of May 21, 2015 giving formal notice to GOOGLE INC.], https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000030746525.

331. Niemela v. Malamas, 2015 BCSC 1024, June 16, 2015 (Can. B.C. S.C.), http://www.canlii.org/en/bc/bcsc/doc/2015/2015bcsc1024/2015bcsc1024.html.

332. Julius Melnitzer, *Google Inc a 'Passive Instrument' of Search Results, B.C. Court Rules*, FINANCIAL POST (July 13, 2015, 3:55 PM), http://business.financialpost.com/legal-post/google-inc-a-passive-instrument-of-search-results-b-c-court-rules.

333. *Id.*

334. Corte Suprema de Justicia [C.S.J.] [Supreme Court], Sala Penal Junio 10, 2015, M.P: J.L. Barceló Camacho, 18837 (Colom.).

335. *Id.* para. 6. *See also* Redacción Judicial, *Coletazos del derecho al olvido* [Death throes

obligation to delist is linked with the right of rehabilitation, and so one may wonder whether this ruling will be applicable in other circumstances.

In Argentina, fears of a "right to be forgotten" are "unfounded," as one scholar points out: "Argentine court judgments favorable to plaintiffs suing Internet search engines have rested on statutory rights of intellectual property, reputation, data protection or privacy. Most of these had to do with the unique Argentine Ley 11.723 for placing a photograph into commerce without authorization." [336] Furthermore, in its subsequent *Da Cunha, Virginia c/ Yahoo de Argentina S.R.L. y otro s/ daños y perjuicios* decision, the Supreme Court of Argentina decided that search engines could not be held responsible for the content individuals and entities decided to publish on their own websites.[337] This ruling was rendered on the basis of the Liability Law and not on the Privacy Law. So this decision is fundamentally different from others discussed in this paper, and if some commentators talked about a "right to be forgotten," this case is not exactly what this paper considers that right to be.

Finally, *Google Spain* had an influence on other jurisdictions or legislatures around the world. However, many rulings are more restrictive and had been made in consideration of a right to rehabilitation or, in some specific circumstances, in consideration of the person who published the content. The right to delisting is sometimes recognized only if the publisher is the plaintiff. Finally, the right to delisting recognized by the CJEU is more powerful. However, the Russian Law merits special attention because the right to delisting is recognized in favor of public persons. It could be dangerous for the freedom of speech and the right to know. Generally speaking, it is necessary to consider the context of the application of the "right to be forgotten."

---

of the Right to Be Forgotten], EL ESPECTADOR (Aug. 31, 2015, 10:24 PM), http://www.elespectador.com/noticias/judicial/coletazos-del-derecho-al-olvido-articulo-582913. This decision follows one by the Constitutional Court in which a woman who had been found innocent of a criminal charge was able to require the newspaper to correct information in its digital edition, and to have the newspaper use technical measures to restrict access to the information (for example, by using robots.txt files and meta-tags to restrict access, assimilated to "privacy by design"), but was not able to obtain an order for delisting by search engines. Corte Constitucional [C.C.] [Constitutional Court], mayo 12, 2015, M.P: M.V. Calle Correa, Expediente T-4296509, Sentencia T-277 de 2015 (Colom.). There are also limits to individual protections when public figures are involved or there are crimes against humanity or human rights violations. *See* Carolina Botero Cabrera, *No habrá 'derecho al olvido' en Colombia*, EL ESPECTADOR (July 2, 2015, 11:23 PM), http://www.elespectador.com/opinion/no-habra-derecho-al-olvido-colombia.

336. Edward L. Carter, *Argentina's Right to be Forgotten*, 27 EMORY INT'L L. REV. 23, 38 (2013).

337. Corte Suprema de Justicia de la Nacion [CSJN] [National Supreme Court of Justice], 30/12/2014, "Da Cunha, Virginia c/ Yahoo de Argentina S.R.L. y otro s/ daños y perjuicios / recurso de hecho", CSJ 561/2010 (46-D) et CSJ 544/2010 (46-D) (Arg.).

2. Nascent Rights: *Right to Obscurity and Right to Digital Oblivion* of Data Collected by Information Society Services

Commenting on then-current discussions among policymakers and stakeholders on reforming the U.S. privacy framework, then-FTC Commissioner Julie Brill said:

> I don't believe a broad EU-style right to be forgotten will be included in these discussions, because the further reaches of a broad right to be forgotten modeled on the CJEU's decision would raise serious questions under the First Amendment here in the US. For that reason alone, I prefer to focus on somewhat more targeted approaches to a right of obscurity that could work here and provided [sic] much needed additional protections to individuals.[338]

The ***right to obscurity*** could be an acceptable form of the "right to be forgotten" in the United States. As Commissioner Brill continued: "Obscurity means that personal information isn't made readily available to just anyone. It doesn't mean that information is wiped out or even locked up; rather, it means that some combination of factors makes certain types of information relatively hard to find."[339] According to Hartzog and Stutzman, "information is obscure online if it lacks one or more key factors that are essential to discovery or comprehension."[340] They identify four of these factors: (1) search visibility; (2) unprotected access; (3) identification; and (4) clarity.[341] They have argued that the "right to obscurity" in Cyberspace should be easier to implement than the difficult to define "right to privacy," and the behaviors that might constitute breach of the right to privacy in Cyberspace: "Obscurity could also serve as a compromise protective remedy: instead of forcing websites to remove sensitive information, courts could mandate some form of obscurity."[342] One may consider that "obscurity is the optimal protection for most online social interactions and, as such, is a natural locus for design-based privacy solutions for social technologies."[343] In the age of big data, it is relevant that the U.S. and the EU are trying to work together even if their concepts of privacy are traditionally different.[344]

338. Selinger & Hartzog, *supra* note 174.

339. *Id.*

340. Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 4 (Feb. 2013).

341. *Id.*

342. *Id.* at 2.

343. Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 385 (2013).

344. *See* Julie Brill, U.S. Fed'l Trade Comm'r, Remarks at Mentor Group Vienna Forum: Privacy in the Age of Omniscience: Approaches in the United States and Europe (Sept. 11, 2014),

The U.S. *Data Broker Accountability and Transparency Act of 2015* bill may be considered a form of the right to obscurity as it would allow consumers to opt out of having their information collected and sold by data brokers for marketing purposes.[345]

Finally, the right to obscurity has less impact than the "right to be forgotten," because the information is not deleted but only made less easy to find. But this right is very interesting, because it could play a more important role in U.S. federal legislation than the "right to be forgotten" which may conflict with the "freedom of speech" clause of the First Amendment of the U.S. Constitution. This right is not yet recognized in law.

Concerning the ***right to digital oblivion*** **of data collected by information society services**, some countries have decided to satisfy the social demand to delete certain personal information collected by information society services. First of all, Nicaragua enacted the Law on Personal Data Protection,[346] and the Regulation of the Law on Personal Data Protection.[347] According to these pieces of legislation, an individual has the right to request that social networks, browsers, and servers suppress or cancel his or her personal information contained in their databases. This is one of the first laws to seek to include the "right to be forgotten." In the case of databases of public and private institutions that offer goods and services and collect personal information for contractual reasons, individuals may request that their personal information be canceled once the contractual relationship ends. This provision is not particularly detailed, and it is not clear how organizations will implement these obligations in practice.[348]

In Europe, Article 17(1) of the GDPR is on the "right to be forgotten" in a digital context:

> The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

https://www.ftc.gov/system/files/documents/public_statements/581751/140911mentorgroup.pdf.

345. S. 668, 114th Cong. § 4(e) (2015).

346. Ley no. 787, 21 Mar. 2012, ley de protección de datos personales [Law on Personal Data Protection], LA GACETA, DIARIO OFICIAL [L.G.] 29 March 2012 (Nicar.), http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d?OpenDocument.

347. Regulation of the Law on Personal Data Protection (Decree No. 36- 2012) Oct. 17, 2012 (Nicar.).

348. *See* Cynthia Rich, *Privacy in Latin America and the Caribbean*, PRIVACY & SECURITY L. REP., 13 PVLR 626, Apr. 14, 2014.

> . . .
>
> (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[349]

This rule complies with the Recommendation made by the Council of Europe in 2012 regarding social networking services:

> [U]sers must be informed about the following: the need to obtain the prior consent of other people before they publish their personal data, including audio and video content, in cases where they have widened access beyond self-selected contacts; how to completely delete their profiles and all data stored about and from them in a social networking service, and how to use a pseudonym. Users should always be able to withdraw consent to the processing of their personal data.
>
> . . .
>
> Upon termination, all data from and about the users should be permanently eliminated from the storage media of the social networking service.[350]

In addition, the GDPR provides for a right of erasure for minors.[351]

The right to oblivion of data collected by information society services is a real right to be forgotten which can be exercised without the condition of providing evidence. It is not necessary to prove that the data are irrelevant, out-of-date, or illegal. Besides, it is not merely a right to obscurity, because the data are deleted. Therefore, it is a broad right to obtain the erasure, meeting a social demand for this right, especially with respect to social network services.

349. *See* GDPR, *supra* note 21, art. 17(1), 17(1)(f), at 43–44.

350. *See* Recommendation CM/Rec(2012)4, *supra* note 305.

351. Article 17(1)(f) of the GDPR should be read together with one of the grounds for this right, that "personal data have been collected in relation to the offer of information society services referred to in Article 8(1)," which covers the case when the services are provided based on consent, and the data subject is less than sixteen years of age, in which case consent must be "given or authorized by the holder of parental responsibility over the child." *See* GDPR, *supra* note 21, art. 8(1), at 37.

II. CRITERIA AND ORGANIZATION OF FORMS OF THE "RIGHT TO BE FORGOTTEN" INTO OUR PROPOSED TAXONOMY

This paper proposes to apply the criteria provided by WP 29 with respect to the right to delisting to the five different variations of the "right to be forgotten" that this paper has identified in its proposed taxonomy. These are set out in the following table. This is a categorization of laws and cases through the use of actual illustrations of each variation of the "right to be forgotten," including some that the authors of this paper have reviewed, but which have not otherwise been detailed in the paper itself.

TABLE: ANALYSIS OF THE "RIGHT TO BE FORGOTTEN" (CRITERIA/CONDITIONS)

CRITERIA	RIGHT TO REHABILITATION (General Context)	RIGHT TO DELETION (PERSONAL DATA LEGISLATION) (General Context)	RIGHT TO DELISTING (Digital Context)	RIGHT TO OBSCURITY (Digital Context)	RIGHT TO DIGITAL OBLIVION (Digital Context)
Where and who?	Examples: • French Law: Criminal Code, Art. 133-12[352] • UK Law: Rehabilitation of Offenders Act[353] • US Law: Fair Credit Reporting Act (FCRA)[354]	Examples: • French Law: Data Protection Act[355] • EU: Data Protection Directive[356] • Europe: Council of Europe Convention 108[357] • US: Specific Federal legislation/Specific State legislation[358]	Examples: • EU: Google Spain Case (case law)[359] • Russia: delisting law[360] • Israel: amendment bill to the Privacy Act (PPA)[361] • Brazil: Bill no. 7881/2014[362]	US: draft Data Broker Accountability and Transparency Act of 2015[363]	• Nicaragua[364] • EU: GDPR and Council of Europe's recommendation[365] • US: California "Erasure Law" in favor of minors[366] • US: State legislation on "revenge porn"[367]
Exercised by whom?	The ex-offender data subject	The data subject	The data subject	The data subject	The data subject

Of general or specific application?	Specific in a context of judicial past in the aim of social rehabilitation	• France, EU, and Asia: general • US: specific	Specific	Specific	Specific
Source?	Criminal Law	Personal data legislation	• Case law in Europe • Case law in certain other countries	Federal law	Law
Limited to a certain age?	No	No	No	No	It could be: California Law on right to be forgotten is limited in favor of minors
Conditions on data?	No	Incomplete, irrelevant, inaccurate, or up-to-date information	Several criteria: not public life, minor, irrelevant, inaccurate, or up-to-date information	Data used in a marketing purpose	• Specific context: data collected by information society services (especially social networks) • Specific content: revenge porn
Absolute right or balancing against other interests?	No, but strict legal conditions	No, but legal conditions on data and evidence	No, but balancing with the freedom of speech	Yes, but only a right to obscurity in a commercial use	Yes, but in specific circumstances

Merely delisting/de-indexing or is original source affected?	Original source is not deleted, but the accessibility is reserved to judges (obscurity in the effect)	Original source is deleted	Delisting and not to the original source	Only obscurity and not deletion of the original source	Original source
Party held accountable for compliance?	The judicial decision must be respected by everyone	Controller and processor	Operator of search engine	Data brokers	Information society service providers
Who decides? Private actors, judge, or administrative authority?	Judge	Controller, administrative authority, or judge	Operator of search engine, administrative authority, and judge	Data brokers and judge	Information society service providers and judge
Party bearing the burden of proof?	Data subject	Data subject	Data subject	Data subject	Data subject
Effects: National effect? Transnational effect?	Transnational effect	National effect	*Debate on this point*[368]	Transnational effect	Transnational effect

352. CODE PENAL art. 133-12 (Fr.), *supra* note 84.

353. Rehabilitation of Offenders Act 1974, c. 53 (Eng.), *supra* note 86.

354. 15 U.S.C. § 1681 (1970), *et seq*., *supra* note 92.

355. French Data Protection Act, *supra* note 16, art. 6(4)–(5), at 9.

356. EU Data Protection Directive, *supra* note 17, art. 6(1), at 40.

357. Convention 108, *supra* note 105, art. 5.

358. *See* 16 C.F.R. § 312 (2015), *supra* note 165; *see also* Selinger & Hartzog, *supra* note 174; and *see* R.I. GEN LAWS 1956 §11-49.3-2(a) (1956), *supra* note 175.

359. Case C-131/12 Judgment of the Court (Grand Chamber), Google Spain SL v. Agencia Española de Protección de Datos, CURIA paras. 89–99 (May 13, 2014) (ECLI:EU:C:2014:317), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX :62012CJ0131.

360. Russian Delisting Law, *supra* note 308.

361. *See* Dan Or-Hof, *supra* note 314.

362. Bill no. 7881/2014, *supra* note 319.

363. S. 668, *supra* note 345.

364. Ley No. 787 (Nicar.), *supra* note 346; Decree No. 36-2012 (Nicar.), *supra* note 347.

365. GDPR, *supra* note 21, art. 17(1), 17(1)(f), at 43–44; Recommendation CM/Rec(2012)4, *supra* note 305.

366. CALIF. BUS. & PROF. CODE § 22581 (2013) (2013 S.B. 568; Chapter 336).

367. For a discussion of some of these State statutes, see Clay Calvert, *Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction*, 24 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 673, 683-699 (2014).

368. There has been a debate on this point following the *Google Spain* decision, with the EU data protection authorities on the one hand, and Google on the other hand. Until recently, Google has taken the view that the decision only requires delisting from EU domain names, thus only has a regional effect, and not a true transnational one (which would pick up generic domains, e.g., ".com"). The CNIL and the other EU data protection authorities have asserted that delisting should be with transnational effect; that is with respect to "all relevant domains, including .com." *See* W. Gregory Voss, *After* Google Spain *and* Charlie Hebdo: *The Continuing Evolution of European Union Data Privacy Law in a Time of Change*, 71 BUS. LAW. 281, 283–284 (2015). Most recently, Google sought to close the debate by geographically filtering search results by the location of the person doing the search, thereby blocking certain results from generic domains when the search was conducted from the EU. In its Decision no. 2016-054 of Mar. 10, 2016 of the Restricted Committee issuing Google Inc. a financial penalty, the CNIL rejected this proposed solution. *See Right to be Delisted: the CNIL Restricted Committee Imposes a €100,000 Fine on Google*, CNIL (Mar. 24, 2016), https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google.

CONCLUSION

The above study of the "right to be forgotten," resulting in a taxonomy of five forms of the "right to be forgotten," appears to reveal a convergence of legal norms whose scope should, however, be measured. Beyond a simple *right to rehabilitation*, many countries today, representing all of the continents of the world, have adopted personal data protection legislation using, more or less, the Data Protection Directive as a model, as encouraged by its Article 25 on cross-border transfers of data to third countries, which requires a finding of an adequate level of data protection of the receiving country if one wants to receive personal data collected in Europe.[369] In other words, an adequate level of data protection, from a European perspective, is necessary from the moment one seeks to establish business relationships with Europe, whether in the digital economy or not, because of the importance of personal data flows.

This paper has shown that many countries grant rights to data subjects whose data are collected, including the right to correction and deletion of the data. However, this *right to deletion* does not automatically pave the way to an interpretation as audacious as that of the CJEU. Thus, it may be seen that Europe remains ahead of countries in other regions in the protection of personal data. This is even truer with the GDPR, which grants a subjective and arbitrary right to have one's personal data deleted by information society service providers, which are the most data-consuming parties.[370] Thus, Europe is keeping one step ahead in the protection of personal data, which it has lifted to the rank of a fundamental right in its Charter. Conversely, it is uncertain whether the arguable "economic opportunism" that some countries may have shown, particularly in Asia or the U.S., in order to allow trade with Europe, reflects a real will to strongly protect individuals. The convergence of legal norms exists on the legal-instrument level but is certainly not as deep as it seems in its normative force.

Furthermore, as we have seen, new forms of the "right to be forgotten" that appear in a digital context—the *right to delisting*, the *right to obscurity*, and the *right to digital oblivion*—result from the willingness to enable individuals to control their image, their reputation, and extend further to all information about them. The idea of a "self-determination"

369. EU Data Protection Directive, *supra* note 17, art. 25, at 45–46.
370. GDPR, *supra* note 21, art. 17, at 43–44.

or "informational self-determination" is emerging from this debate of late.[371] The individual right to control one's profile and data today is reflected in concrete terms by the GDPR, which recognizes the right to remove data that one no longer wants to have appear on information society services.[372] One may also wonder if the operators of services are not trying to adapt, at least partially, to this new trend, enabling individuals to manage their data and services, such as Google has done with *My Account*. The *policies* of stakeholders will have to adapt and the provision of simple technical tools to individuals could be more effective.

Finally, this study of the "right to be forgotten" and the taxonomy of its various forms should be considered more generally as a way to reflect on the evolution of privacy and data protection in Europe, the U.S., and elsewhere, and to discuss certain rights in a clear fashion, using a standardized terminology. But whether this reconciliation of legal norms is voluntary or forced, it becomes inevitable in a globalized digital economy based on the flow of information.

371. *See* Conseil d'Etat [Council of State], Summary: Digital Technology and Fundamental Rights (Annual Study (2014)), (Fr.), http://www.conseil-etat.fr/content/download/33163/287555/version/1/file/Digital%20technology%20and%20fundamental%20rights%20and%20freedoms.pdf.

372. GDPR, *supra* note 21, art. 17, at 43–44.