Kentucky Law Journal

Volume 103 | Issue 3 Article 2

2014

Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten

Lawrence Siry
University of Luxembourg

Kentucky Law Journal

VOLUME 103 2014-2015 NUMBER 3

ARTICLES

Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten

Lawrence Siry[1]

ABSTRACT

In May of 2014, the Court of Justice of the European Union handed down its decision in the case of Google Spain SL v. Agencia Española de Protección de Datos.[2] *This landmark decision ignited a firestorm of debate over the "right to be forgotten": the right of users to withdraw information about themselves available on the internet. With concerns about the restriction of the freedom of expression on the internet, many commentators have criticized the decision as unworkable and dangerous. Others have recognized continuity in the development of privacy and data protection jurisprudence within the European courts. Meanwhile in Brussels, the European Union (EU) has been crafting a new data protection regulation, which will apply to its twenty-eight Member States. This new regulation will more than likely extend the concept of some form of the "right to be forgotten," or more precisely, a right to erasure of material on the internet.*

This paper will explore the basis and impact of the Google Spain decision. Beginning with an exploration of the theoretical underpinnings of the "right to be forgotten" in Europe, the paper will attempt to reconcile the conceptualization of this privacy right with the privacy framework existing

[1] Lawrence Siry is a Collaborateur de Reserche in the Faculty of Law, Economics and Finance at the University of Luxembourg. Mr. Siry holds a PhD in Law from the University of Luxembourg and is an attorney licensed to practice in the State of New York. The research for this article was conducted while Mr. Siry did his post-doctoral research at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg. The author would like to thank Mathilde Stenersen and Jenny Metzdorf for their contributions to this article.

[2] Case C-131/12, Google Spain SL Google, Inc. v. Agencia Española de Protección de Datos (AEPD) (E.C.J. May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang-EN&docid=152065.

in the United States. It will then turn to proposals for legislation from both sides of the pond to assess what they will and will not potentially achieve. The paper will consider the European Union rules in light of the current framework and the proposed reforms, comparing European and American provisions, specifically California Law and proposals pending before the United States Congress. Are these measures the silver bullet that privacy advocates hope for, or will they open a Pandora's box of excessive Internet censorship that will cause the destruction of history? Are the two theoretical frameworks compatible, signalling a convergence of policies towards a more privacy oriented legal structure? To this end, the practical application of the proposed rules, their effectiveness, and their efficacy will be examined.

INTRODUCTION

Comparatively, it is evident that the concept of privacy in the United States differs greatly from that in Europe. The expectations of the citizenries differ as well. Even as Europe and North America become increasingly interconnected through technology, the instantaneous dissemination of news, information, culture, and ideas, the neighbors across the pond differ substantially in their opinions on what information ought to be considered private, how personal information ought to be protected, what power individuals have in controlling information about them on the internet, and what role government ought to play in the process.

With the dominance of American companies in the information technology (IT) sector, it is impossible to effectively consider data protection regulation without considering the American cultural perspective.[3] Yet European political and judicial decisions have created a sense of a right that does not always match these American perspectives.[4] Reaching a common understanding is necessary as users and policymakers seek to maximize the efficiency and continuity of the global market.[5] One area that has proven to be both popular and controversial in the European setting is the fabled "right to be forgotten." Almost utopian in scope, it would allow cybercitizens to start fresh after a brush with the law, or to forget those embarrassing, somewhat impetuous photos that one posed for back in one's

[3] *The Software and Information Technology Services Industry in the United States*, SELECT USA, http://selectusa.commerce.gov/industry-snapshots/software-and-information-technology-services-industry-united-states (last visited Feb. 12, 2015).

[4] Alistair Barr & Sam Schechner, *Google Advisory Group Recommends Limiting 'Right to Be Forgotten' to EU*, WALL ST. J. (Feb. 6, 2015 3:35AM), http://www.wsj.com/articles/google-advisory-group-says-limit-right-to-be-forgotten-to-eu-1423206470.

[5] Currently, negotiations are ongoing between the United States and the European Union surrounding the domain of data protection. *See* Press Release, European Comm'n, EU-US Data Protection Agreement Negotiations: Frequently Asked Questions (May 26, 2010), *available at* http://europa.eu/rapid/press-release_MEMO-10-216_en.htm?locale=en; EUROPEAN COMM'N, FACTSHEET EU-US NEGOTIATIONS ON DATA PROTECTION, (2014), http://ec.europa.eu/justicia/data-protection/files/factsheets/umbrella_factsheet_en.pdf.

carefree youth.[6] Moreover, it would even allow for past failed business schemes to rest quietly, where they might belong, in the past.[7] In many ways, this "right to be forgotten" is a right derived from the pre-digital era. Newspapers tended to rot and photographs faded or got lost with the passage of time. Business acumen was judged on a current scale rather than one that relied too heavily on ancient memory. Time truly did heal most wounds.

In many respects, the American dream is grounded in a "right to be forgotten": the idea that an individual of whatever stripe could land on the American shore to begin anew. Reinvention was a key attribute of the new world. Yet, with the invention and pervasiveness of the internet, things have truly changed. The internet never forgets, or at least, that is our assumption and our fear.

On the European stage, the Court of Justice of the European Union (CJEU) entered the fray on the 13th of May, 2014 with its long awaited ruling in *Google Spain*,[8] which changes the terrain of online privacy and the ability of citizens to be forgotten. The ruling has the potential to vastly alter the discussions both with regard to legislation being considered by the European Union, as well as the business model employed by Internet related firms such as Google and Facebook.[9]

In the sections that follow, this paper will examine the conceptualization of the right to privacy, which is the underpinning of the "right to be forgotten" in Europe and the U.S. Focusing on legislation and proposed legislation in these two jurisdictions, the paper will attempt to find the common ground between the two regimes. The paper will also examine the potential impact of *Google Spain*. Lastly, the paper will attempt to determine if the "right to be forgotten" is truly necessary or whether it's a gimmick that will have little impact on the core rights of privacy and expression.

---

[6] *See* Tessa Mayes, *We Have No Right to be Forgotten Online*, THE GUARDIAN (Mar. 18, 2011, 10:16 AM), http://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet ("[A] right to be forgotten is about extreme withdrawal, and in its worse guise can be an antisocial, nihilist act. If enacted, a right to be forgotten would signify the emasculation of [the European Union's] power to act in the world."); *see also* Danny Hakim, *Right to be Forgotten? Not that Easy*, INT'L N.Y. TIMES, May 29, 2014, http://www.nytimes.com/2014/05/30/business/international/on-the-internet-the-right-to-forget-vs-the-right-to-know.html.

[7] *See* Hakim, *supra* note 6 ("[T]he tech industry has portrayed the decision as a blow against the free flow of information on the web and a victory for those who want to cover up past misdeeds —including pedophiles, corrupt politicians and unscrupulous businesspeople.").

[8] *Google Spain*, Case C-131/12.

[9] *See generally Essential Guide: EU Data Protection Regulation*, COMPUTER WKLY., http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you (last visited Feb. 8, 2015); European Comm'n, *Protection of Personal Data*, http://ec.europa.eu/justice/data-protection (last updated Sept. 4, 2014).

I. THE EUROPEAN RIGHT TO BE FORGOTTEN

A. The Basis for the Right: European Privacy and Data Protection

In order to fully appreciate the development of the "right to be forgotten" in Europe, it is necessary to take a step back and briefly look at the development of fundamental rights in a pan-European context, particularly the right to privacy, or private life, since the "right to be forgotten" derives from privacy rights and data protection legislation.

Fundamental rights in Europe are protected not only by national constitutional paradigms, but also by pan-European structures. After the Second World War, western democracies founded the Council of Europe and signed the European Convention on Human Rights (ECHR).[10] Rooted in the determination to never repeat the rights abuses of the past, contracting states established minimum principles that all citizens could rely upon.[11] The Convention included *inter alia*, the rights to life, fair process, privacy, and the freedom of expression.[12] Perceived violations of these rights can be brought before the European Court of Human Rights (ECtHR).[13] Additionally, contracting states have an obligation to protect their citizens from intrusions against these rights by third parties.[14] With the democratization of Europe, particularly following the fall of the Berlin Wall in 1989 and the end of the Cold War, the Council of Europe has expanded to include forty-seven European nations.[15]

Contrastingly, the European Union began in 1950 as an economic agreement between the nations that comprised the European Coal and Steel Community: France, Germany, Luxembourg, Belgium, the Netherlands, and Italy.[16] The purpose of this union was to avoid another European war by bringing the means of production of the instruments of war under shared management.[17] Alongside treaties designed to bring atomic energy into a common management scheme, as well as the beginning of a common market for the Member States, what would become the European Union began as an economic, rather than political union.[18]

---

[10] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR], *available* at http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[11] *See* Aisha Gani, *What is the European Convention on human rights?*, THE GUARDIAN (Oct. 3, 20140, 10:48 AM), http://www.theguardian.com/law/2014/oct/03/what-is-european-convention-on-human-rights-echr; *see generally* ECHR, *supra* note 10.

[12] *Id.* arts. 2, 6, 8, 10, at 224, 228, 230.

[13] ECHR, *supra* note 10, art. 5, 19.

[14] *See generally Id.*

[15] Matthias Bieri, *The Council of Europe: Time for Reform*, STRATFOR (May 28, 2013, 7:43 AM), https://www.stratfor.com/the-hub/council-europe-time-reform.

[16] *The History of the European Union*, EUROPEAN UNION, http://europa.eu/about-eu/eu-history/index_en.htm (last visited Feb. 8, 2014).

[17] *Id.*

[18] *How the EU Works*, EUR. UNION, http://europa.eu/about-eu/index_en.htm (last visited Feb. 16, 2015).

With the passage of time, ties (both economic and political) have grown and, through a series of treaties, so has membership in the Union. Today there are twenty-eight Member States of the European Union, all of which are contracting states to the European Convention on Human Rights.[19]

In 2009, the enactment of the Treaty of Lisbon effectuated constitutional (or primary) law within the European Union.[20] Under the Treaty of Lisbon, the European Union Charter of Fundamental Rights (the Charter), a primary source of human rights in the European Union, became legally binding.[21] The Charter was proclaimed in 2000 when the Treaty of Nice was adopted, yet its legal value was originally unclear. While many of the rights contained in the European Convention on Human Rights and the Charter are similar, the Charter is more specific in terms of both privacy and data protection rights.[22]

The CJEU, located in Luxembourg, is the arbiter of the interpretation of treaties of the European Union. In areas where the Luxembourg Court interprets rights under the Charter, it follows the jurisprudence of the European Court of Human Rights.[23]

In the European Union, the right to data protection stems from the right to privacy as set out in Article 8 of the European Convention on Human Rights,[24] as well as Article 7 (the right to private life) and Article 8 (the right to the protection of personal data) of the European Union Charter.[25] Primarily, these rights emanated from the right to maintain a private life that the State could not unduly interfere with.

Since the entry into force of the Treaty of Lisbon in 2009, the CJEU has only recently been authorized to apply the Charter in a meaningful fashion. The

---

[19] *See How the EU Works: EU Member Countries,* EUR. UNION, http://europa.eu/about-eu/countries/member-countries (last visited Feb 16, 2015); *see also Development of the European Convention on Human Rights and Fundamental Freedoms, 1950,* MIGRATION CITIZENSHIP EDUCATION, http://migrationeducation.de/28.2.html?&rid=32&cHash=e1406ce90478dac99328adbd62782641 (last visited Feb. 16, 2015).

[20] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter Treaty of Lisbon].

[21] *EU Charter on Fundamental Rights,* EUR. COMM'N, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (last visited Feb. 17, 2015).

[22] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 [hereinafter EU Charter].

[23] Ditlev Tamm, *The History of the Court of Justice of the European Union Since its Origin, in* THE COURT OF JUSTICE AND THE CONSTRUCTION OF EUROPE: ANALYSES AND PERSPECTIVE ON SIXTY YEARS OF CASE LAW 9, 14 (Asser Press, 2013).

[24] 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. ECHR, *supra* note 10, art. 8, at 230.

[25] EU Charter, *supra* note 21, arts. 7–8, at 393.

ECtHR, however, has developed robust jurisprudence protecting privacy.[26] Under rulings handed down by the ECtHR, the right to privacy is vast and affords a broad spectrum of protections, including: relationships within families, the rights of persons to choose sexual partners, the rights of persons to be free from certain types of surveillance, the rights of persons (including celebrities) to be free from intrusion into their private sphere, as well as the right of convicted persons to re-integrate into society after serving a criminal penalty.[27] In 1992, the ECtHR attempted to define the right to privacy, stating:

> "[I]t would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."[28]

The right to privacy is also a right that must be balanced against other rights such as the freedom of expression. The Court's test for determining whether there has been a violation of the right to privacy begins with an inquiry into whether the right has been interfered with.[29] Next the Court determines whether there was a basis in law for the action that was taken.[30] The Court then looks to see whether the interference promoted a legitimate governmental aim and whether it was necessary in a democratic society.[31] The Court does give governments a margin of appreciation in their actions, which is designed to take into account the complexity of historical and cultural differences that exist amongst the contracting states.[32] The right to private life is a positive right, requiring governments of contracting states to protect citizens from intrusion on the right by outside actors.[33]

---

[26] *See, e.g.*, Smith & Grady v. United Kingdom, 29 Eur. H.R. Rep. 493 (2000) (holding that the discharge of personnel from the Royal Navy on the basis of their homosexuality was a breach of their right to private life under Article 8 of the ECHR).

[27] *See, e.g.*, Smith & Grady v. United Kingdom, 29 Eur. H.R. Rep. 493 (2000) (holding that the discharge of personnel from the Royal Navy on the basis of their homosexuality was a breach of their right to private life under Article 8 of the ECHR).

[28] Niemietz v. Germany, 251 Eur. Ct. H.R. (ser. A) 23, para. 29 (1992).

[29] *See, e.g.*, *Smith & Grady*, 29 Eur. H.R. Rep. at paras. 70–80; *see also* A, B & C v. Ireland, 2032 Eur. Ct. H.R. paras. 216–241 (2010), *available at* http://www.bailii.org/eu/cases/ECHR/2010/2032.html.

[30] *A, B & C*, 2032 Eur. Ct. H.R. at paras. 216–241.

[31] *Id.*

[32] Monica Lugato, *The "Margin of Appreciation" and Freedom of Religion: Between Treaty Interpretation and Subsidiarity* 52 J. CATHOLIC LEGAL STUD. 49, 51-52 (2013) (noting that recognition of the "margin of appreciation" has developed because "historical and cultural variations [among Member States] must be taken into account.")

[33] *See, e.g.*, Jean-Francois Akandji-Kombe, *Positive Obligations Under the European Convention on Human Rights: A Guide to the Implementation of the European Obligations Under the European Convention on Human Rights*, COUNCIL OF EUROPE (2007), http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-07 (2007).pdf (discussing the "positive obligation" of the right to a private life that is free from interference from outside actors).

Over time, the right to privacy evolved to include personal data. In cases such as *Leander v. Sweden*[34] and *S & Marper v. United Kingdom*,[35] the ECtHR determined that this right to privacy includes the protection of information relating to a person—a right to protection of personal data—specifically from the supervision and surveillance of States.

While the ECHR dealt primarily with the protection of privacy, which then evolved to include protection of personal data, during the 1980s, the members of the Council of Europe specifically designed legislation to deal with the rise of information technology and processing abilities and the impact it had in terms of protecting citizens' personal data. With the growth and expansion of information technology in the 1960s and 1970s,[36] it became evident that binding rules were required to ensure effective protection. Accordingly, the Council of Europe enacted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108),[37] the first pan-European data protection legislation. Convention 108 sought to "secure . . . for every individual . . . respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data."[38]

Against this backdrop, the European Union crafted Directive 95/46/EC ("the Data Protection Directive" or "DPD") concerning the protection of individuals with regard to the processing of personal data and the free movement of such data.[39] While the European Union sought to find a measure addressing the mounting processing powers and their increasingly global scale,[40] the major thrust behind the Data Protection Directive was the harmonization of the internal market.[41]

Enacted under Article 100 of the Treaty Establishing the European Community of the European Union (EC Treaty),[42] which was concerned with the introduction of measures for the proper functioning of the internal market, the

---

[34] Leander v. Sweden, 116 Eur. Ct. H.R. 3, para. 48 (1987).

[35] S & Marper v. United Kingdom, 48 Eur. H.R. Rep. 50 (2008).

[36] *See* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 15–16 (2014) [hereinafter HANDBOOK], *available at* http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

[37] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 1, Jan. 28, 1981, E.T.S. No. 108 [hereinafter Convention 108], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[38] *Id.* While the majority of signatories are Council of Europe members (forty-five out of forty-six signatories), it is equally open to other nations, with Uruguay becoming the first non-European signatory in 2013. HANDBOOK, *supra* note 36, at 17.

[39] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data art. 3, 1995 O.J. (L 281) 31, 39 [hereinafter Directive 95/46].

[40] Andrew Charlesworth, *Clash of the Data Titans? US and EU Data Privacy Regulation*, 6 EUR. PUB. L. 253, 254 (2000).

[41] HANDBOOK, *supra* note 36, at 18; DOUWE KORFF, DATA PROTECTION LAWS IN THE EUROPEAN UNION 8 (Richard Hagle ed., 2005).

[42] Treaty Establishing the European Community art. 100, Aug. 31, 1992, 1992 O.J. (C 224) 6, 34.

DPD became intrinsically linked to the efficiency of the internal market.[43] With the exploitation of personal data becoming an important feature of the Internet economy, cross-border data flows became more prevalent. The general consensus was that uniformity was necessary to ensure the growth and evolution of the internal market to enable online economic activity.[44] Additionally, for Internet services to become fully economically viable within the European Union, data subjects needed to feel protected. Therefore, guarding their privacy became an imperative for the success of the internal Internet market.[45]

The adoption of the DPD, however, faced a rocky road, as it would harmonize an area so thoroughly embedded in Member States' national law and, in many instances, in their own Constitutions.[46] At the time of its inception, several Member States had already introduced mechanisms for data protection.[47] These safeguards were hardly uniform, however, and ranged in scope and application.

The understanding of data protection as a fundamental right rather than a right linked inextricably to the internal market was enhanced through the adoption of the Treaty of Lisbon.[48] Data protection was offered a greater foundation in European Union law through the incorporation of the European Charter of Fundamental Rights in primary European Union law[49] and by the introduction of Article 16 in the Treaty on the Functioning of the European Union (TFEU).[50] The fundamental status of data protection following these changes elevated the importance of a robust and coherent data protection regime throughout the European Union. The Directive brought together the Member States' varying levels of protection to create legal uniformity in the European Union in terms of data protection laws, which served to further the objectives of the internal market.[51]

However, the Data Protection Directive has its limitations. It applies exclusively to natural persons—not to legal persons—where their activities are carried out in the course of a purely personal or household activity.[52] Furthermore, it does not apply to areas of criminal law, as defined by each Member State, nor

---

[43] Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SECURITY REP. 508, 512 (2008).

[44] SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 91–92 (Raf Casert trans., 2002).

[45] *Id.*

[46] *See* Chris Jones, *National Legal Challenges to the Data Retention Directive*, EU LAW ANALYSIS (Apr. 8, 2014), http://eulawanalysis.blogspot.com/2014/04/national-legal-challenges-to-data.html.

[47] *Id.* at 87.

[48] Treaty of Lisbon, *supra* note 20, at 32, 51.

[49] EU Charter, *supra* note 21, art. 8(1), at 393 ("Everyone has the right to the protection of personal data concerning him or her.").

[50] Consolidated Version of the Treaty on the Functioning of the European Union art. 16(1), May 9, 2008, 2008 O.J. (C 115) 47, 55 [hereinafter TFEU] ("Everyone has the right to the protection of personal data concerning them.").

[51] *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1988 (2013) (noting that "the EU has long been interested in the free flow of personal information and trade in [data] as part of the development of a vibrant internal market").

[52] *See* Council Directive 95/46, 1995 O.J. (L 281) 31, 31.

does it apply to matters of State security.[53] In fact, the entirety of Titles V and VI of the TEU—which cover the areas of freedom, security, justice, and police and judicial cooperation in criminal matters—are outside the scope of the Directive, meaning that both State security matters and criminal law matters on the European Union and national level are excluded.[54] In addition, the European Court of Justice has held that the right to data protection is not an exclusive right, but rather a limited right that must be balanced against other fundamental rights.[55]

In terms of the "right to be forgotten," the European Union data protection framework offers several possible avenues to assert the right to have certain personal data excluded. One such avenue is Article 6 of the Data Protection Directive 95/46, which states that data must be *accurate* and *up to date* or otherwise be erased or rectified[56] and should only be kept identifiable for as long as it is *necessary for the purposes for which it was collected* or further processed.[57] Arguments have been made that this latter provision is somewhat "useless in practice," because in the constantly evolving world of online marketing, "personal data is permanently collected and used for never-ending purposes."[58] The Article 29 Working Party (an independent, advisory committee to the EU's European Commission made up of representatives from each EU member State Data Protection Agency, as well as representatives of EU institutions and the EU Commission) has attempted to rectify this through its Opinion on Purpose Limitation, in which it stresses the need for compatible further use of data with the primary purpose.[59] The Opinion relies on examples such as "online marketing," and states that any description of the purposes for data collection cannot be defined too broadly, but must correctly inform the data subjects of the intentions behind said purposes.[60] Nevertheless, the Opinion also acknowledges that with layered privacy notices, data controllers may further process data.[61]

Furthermore, if data processing is based on consent, any further processing—unless based on another reason—would not comply with the DPD after a subject

---

[53] *Id.* art. 4, at 39.

[54] *Id.*

[55] *See* Joined Cases C-465/00, C-138/01 & C-139/01, Rechnungshof, Neukomm, Lauermann v. Österreichischer Rundfunk, 2003 E.C.R. I-5014, I-5042.

[56] Council Directive 95/46, art. 6, 1995 O.J. (L 281) 31, 40.

[57] *Id.*; *see also* Jef Ausloos, *The 'Right To Be Forgotten' – Worth Remembering?*, 28 COMPUTER L. & SECURITY REV. 143, 149–150 (2012); Richard Jones & Dalal Tahri, *An Overview of EU Data Protection Rules on Use of Data Collected Online*, 27 COMPUTER L. & SECURITY REV. 630, 633 (2011).

[58] Ausloos, *supra* note 57, at 150.

[59] *See generally Opinion 03/2013 of the Data Protection Working Party on Purpose Limitation*, at 23–27 (Apr. 2, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (discussing the different factors that should be considered when determining whether further processing is compatible and allowed under the Directive).

[60] *See id.* at 15–16.

[61] *See id.* at 16.

withdraws consent.[62] While it might be argued that the withdrawal of consent does not apply to any past processing activities and is only applicable to future processing activities, withdrawing consent for a specific set of data—even past data—should entail an end to processing. For example, deleting a picture on a social networking account might be considered withdrawing consent for further processing, as the social network user no longer wishes for the picture to be available. If the picture is deleted—i.e. consent is withdrawn—it is no longer possible for the data controller to process the data and it should be removed, since even storing the data qualifies as processing it.[63] Additionally, the Article 29 Working Party has posited that a data subject should always be allowed to withdraw his/her consent.[64] However, there is no specific provision for this in the DPD nor an overt requirement to delete data after the data subject has chosen to withdraw consent, making the reliance on this particular right somewhat troublesome.[65]

There is a requirement to delete data in Article 12(b) of the DPD, which provides for "the [right to] rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[66] The application of these provisions, however, is not entirely clear due to the specification that the data be incomplete or inaccurate.[67] Also, because the DPD provides that "rectification, erasure *or* blocking"[68] should be employed "as appropriate," erasure may not always be the chosen route to handle the "incomplete or inaccurate nature of the data."[69] Where consent has been withdrawn or the data is no longer needed for the purposes for which it was collected, erasure of the data could follow, as processing would no longer comply with the requirements of the DPD.[70] If the data subject wishes to exercise this right, it would be up to the controller to prove that the processing is legitimate.[71]

---

[62] *Opinion 15/2011 of the Data Protection Working Party on the Definition of Consent*, at 9 (July 13, 2011), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

[63] *See* Council Directive 95/46, art. 2, 1995 O.J. (L 281) 31, 38 ("'[P]rocessing of personal data' . . . shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction . . . .").

[64] *Opinion 15/2011*, *supra* note 62, at 9; *see* Paul Bernal, *The EU, the US and the Right To Be Forgotten*, *in* RELOADING DATA PROTECTION: MULTIDISCIPLINARY INSIGHTS AND CONTEMPORARY CHALLENGES 61, 62 (Serge Gutwirth et al. eds., 2014) (arguing that the individual's right to withdraw consent is protected under the existing data protection regime).

[65] Meg Leta Ambrose & Jef Ausloos, *The Right to be Forgotten Across the Pond*, 3 J. INFO. POL'Y 1, 7 (2013); *see* HANDBOOK, *supra* note 36, at 60.

[66] Council Directive 95/46, art. 12, 1995 O.J. (L 281) 31, 42.

[67] *See id.*

[68] *Id.* (emphasis added).

[69] *Id.*

[70] HANDBOOK, *supra* note 36, at 111.

[71] *Id.*

Article 14(a) of the DPD also offers data subjects the possibility to object to processing, subject to a very specific and narrow set of requirements.[72] Member States must grant a right to object where processing is based on Article 7(e)—"processing . . . for the performance of a task carried out in the public interest"—or Article 7(f)—"processing . . . for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed."[73] Furthermore, the data subjects may only object on a "compelling legitimate ground" relating to their "particular situation" to the processing of data relating to them.[74] So, in cases where the data subjects have consented, where the processing is necessary to perform a contract, where the procession meets a legal obligation, or where the procession protects a vital interest of the data subject, the Member State need not offer a right to object.[75] One clear option to prevent processing is through Article 14(b) by which data subjects are always empowered to object to processing without needing justification as long as the data will be used for direct marketing purposes, or following notification of data disclosure to third parties.[76]

In theory, therefore, the DPD provides for several avenues for data erasure. However, as noted, the application of these options is somewhat flawed. Attempts to have online personal data deleted can be found in various Member States, with the most notorious example probably being the German Sedlmayr case.[77]

In 1990, Wolfgrang Werlé and Manfred Lauber were convicted of the murder of Walter Sedlmayr, a famous actor.[78] Due to the high-profile status of the victim, news reports and articles about the two killers flourished, resulting in a number of articles about the two available online.[79] After they had served lengthy sentences for Sedlmayr's murder, Werlé and Lauber sued publishers for the removal of information from various websites about their involvement as they felt it would negatively impact their lives after imprisonment.[80] They sought to delete the data about them online by relying on their personality rights.[81] German law states that "true statements may violate personality rights, when they are likely to have a negative effect on the person or his reputation, which is disproportionate to the interest of disseminating the truth," particularly where statements have a potentially large audience and can lead to the social exclusion of the person.[82] While the two men were successful in the lower courts, the German Federal Court held that "as

[72] Council Directive 95/46, art. 14, 1995 O.J. (L 281) 31, 42.

[73] *Id.* arts. 7, 14, at 40, 42–43.

[74] *Id.* art. 14, at 42–43.

[75] Ambrose & Ausloos, *supra* note 65.

[76] Council Directive 95/46, art. 14(b) 1995 O.J. (L 281) 31, 43.

[77] *See* Bundesgerichtshof [BGH] [Federal Court of Justice] July 21, 1994, 40 ENTSCHEIDUNGEN DES BUNDESGERICHTSHOFES IN STRAFSACHEN [BGHST] 211, 1994 (Ger.).

[78] Lawrence Siry & Sandra Schmitz, *A Right To Be Forgotten? - How Recent Developments in Germany May Affect the Internet Publishers in the US*, 3 EUR. J. L. & TECH., no. 1, 2012, at 1, 3.

[79] *Id.*

[80] *Id.* at 3–4.

[81] John Schwartz, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, N.Y. TIMES (Nov. 12, 2009), http://www.nytimes.com/2009/11/13/us/13wiki.html.

[82] *Id.* at 4.

long as the archived story does not give the impression that it is up to date or presents an afresh publication on the offender or has the characteristics of an afresh publication, the provision of the story in an online archive is legal."[83] With regard to the relatively easy access to the stories by search engines, the Court determined that the fact that the service facilitated finding older stories did "not constitute sufficient reason to eliminate our 'historical memory.'"[84] The personality rights in Germany were, thus, not sufficient to eliminate the value of data retained online about the pair and their crime.[85]

On the heels of the Sedlmayr case, the Italian courts faced similar issues. In 2010, an Italian court found Google executives guilty of violating Italian privacy law because they failed to remove from the Google Italia Video service a video of a disabled boy being bullied.[86] The executives have since been acquitted by the Italian Supreme Court which found that, as a hosting provider under the e-Commerce Directive,[87] Google could not be considered liable absent knowledge or notice.[88]

B. Google Spain SL v. Agencia Española de Protección de Datos

In 2012, the Spanish data protection authority brought before the Court of Justice of the European Union a case that is currently garnering substantial attention.[89] The case centered on the extent to which the Data Protection Directive applies to Internet search engines and the extent of the application of the "right to be forgotten."[90]

---

[83] *Id.* at 5.

[84] *Id.*

[85] The UK witnessed a similar, though more nefarious, incident regarding two ten-year-olds abducting, torturing, and killing a two-year-old. Both were put in juvenile detention, but rather than relying on data protection to prevent information about them spreading, the chosen course of action instead was to issue an injunction after the trial against any publication of information relating to the identity and location of the boys. The injunction was maintained after their release to protect their new identities. Speculation as to their whereabouts and identities persist and a number of cases regarding the breach of the injunction have been heard with resulting suspended sentences. Yet, dedicated Wikipedia cases and news articles persist. *See, e.g.*, *Murder of James Bulger*, WIKIPEDIA, http://en.wikipedia.org/w/index.php?title=Murder_of_James_Bulger&oldid=632422899 (last modified Nov. 4, 2014). As will be seen in the sections that follow, a real question would be whether the German courts (or for that matter, any national court in the EU) would decide the case similarly after the *Google Spain* case.

[86] *See* Jon Brodkin, *Italy Finally Acquits Google Execs Convicted over User-Uploaded Video*, ARSTECHNICA (Dec. 21, 2012, 3:28 PM), http://arstechnica.com/tech-policy/2012/12/italy-finally-acquits-google-execs-convicted-over-user-uploaded-video.

[87] Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market art. 14, 2000 O.J. (L 178) 1, 13.

[88] *See, e.g.*, Giulio Coraggio, *Google Vividown Case Sets New Rules on Internet Liability*, DLA PIPER IPT ITALY BLOG (Feb. 17, 2014), http://blogs.dlapiper.com/iptitaly/google-vividown-case-sets-new-rules-on-internet-liability.

[89] Case C-131/12, Google Spain SL Google, Inc. v. Agencia Española de Protección de Datos (AEPD) (E.C.J. May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang-EN&docid=152065.

[90] *Id.* paras. 1–2.

In the *Google Spain* case, Costeja González, a Spanish citizen wished to remove information related to an auction of his real estate due to social security debts from an online newspaper archive.[91] The publisher of the newspaper, *La Vanguardia*, refused the request, stating that the publication of the information was not only legal, but mandated by a state institution.[92] In response, Costeja González contacted Google to have the links to the information removed.[93]

In 2010, Costeja González filed a complaint with the Spanish Data Protection Agency, *Agencia Española de Protección de Datos* (AEPD), against both the newspaper and Google Spain, claiming that the retention of the material on the internet amounted to a violation of his rights under the Spanish transposition of the Data Protection Directive.[94]

The AEPD dismissed the complaint against *La Vanguardia*, holding that "the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible."[95] To the contrary, the AEPD found that operators of search engines, such as Google Spain, are subject to data protection legislation since they act as intermediaries and are responsible for the data they process.[96] As such, the AEPD found that it had the authority to require Google to remove access to certain information that would violate national data protection laws and the principles of Articles 7 and 8 of the European Union Charter, protected therein.[97]

Google Spain brought an action in Spanish courts to annul the decision of the AEPD. The Spanish court in turn referred the question of interpretation of European law to the Court of Justice of the European Union.[98]

A fundamental issue that the Court addressed was whether search engines could be considered "controllers" of data.[99] If yes, they would be subject to the DPD as transposed by national law.[100] Contrastingly, if search engines were found to be mere intermediaries of data dissemination, then they would not be subject to the regulations of the DPD.[101] Relying on previous jurisprudence, the Court

---

[91] *Id.* para. 14.

[92] *Id.* para. 16.

[93] *Id.* para. 15.

[94] *Id.* paras. 14, 23.

[95] *Id.* para. 16.

[96] *Id.* para. 17.

[97] *Id.* para. 17.

[98] Under Article 267 of the Treaty on the Functioning of the European Union, a vast majority of the cases before the Court are requests by national courts for a Preliminary Ruling on an interpretation of European Law, rather than a determination of the specific facts of the case. The interpretation, however, as in the case of *Google Spain*, can determine the outcome of the national proceedings. TFEU, *supra* note 50, art. 267, at 164.

[99] *Google Spain*, Case C-131/12, at para. 20(2)(b).

[100] *See* Council Directive 95/46, art. 6(2), 1995 O.J. (L 281) 31, 40 ("It shall be for the controller to ensure that [the principles relating to data quality are] complied with.").

[101] *See Id.*

quickly found that "the operation of loading personal data on an Internet page must be considered to be such 'processing'"[102] within the meaning of the Directive:[103]

> "[I]t must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves,' 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data."[104]

The Court went on to find that search engines have a significant effect on fundamental rights to privacy and the protection of personal data.[105] As actors independent of the original publisher of the material, search engines determine what material will be available to the Internet-using public.[106] This is especially true in light of current technology, which enables operators of search engines to exclude certain materials from search results at the request of publishers.[107]

Ultimately, the Court held that the "right to be forgotten" is not absolute.[108] Instead, it requires a balancing between the interest of privacy and the significance of the information at issue.[109] This balancing potentially pits the right to privacy against the freedom of expression and/or the right to receive information. Where the controller determines that the interest of privacy does not rise to a level requiring the link to the information to be severed, the Court held that either the data protection authority, or a court, would be best suited to determine the appropriate balance.[110]

Interestingly, the Court held that it is not just inaccurate information that might be forgotten.[111] True and accurate material, which may be "inadequate,

---

[102] *Google Spain*, Case C-131/12, at para. 26.

[103] The DPD defines "controller" in Article 2 as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law." Council Directive 95/46, art. 2, 1995 O.J. (L 281) 31, 38. The DPD also defines "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." *Id.*

[104] *Google Spain*, Case C-131/12, para. 28.

[105] *Id.* para. 38.

[106] *Id.* paras. 38–39.

[107] *Id.* paras. 39–40.

[108] *Id.* paras. 73–74.

[109] *Id.* paras. 74–76.

[110] *Id.* para. 77.

[111] *Id.* paras. 72, 92.

irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes," are also subject to the ruling.[112]

In its final analysis, the Court rejected the argument that a search engine is a mere conduit of information and therefore not subject to the rules governing data processing and the control of content.[113] The Court held that links are critical to the analysis because the links that a search engine regulates control the information that an end user receives.[114] Therefore, the Court found that Google was subject to European (and therefore Spanish) data protection rules.[115] As such, the right to impart such information as protected by Article 10 ECHR, must be balanced against the subject's right to private life and data protection as afforded by Article 8 ECHR and Articles 7 and 8 of the Charter. As material not of particular historical or scientific import ages, its Article 10 value diminishes while its potential for damage in light of Article 7 (privacy) may grow. Post-*Google Spain*, search engines are now required to balance these various interests against each other.[116]

The *Google Spain* decision will undoubtedly influence the legislation machine currently crafting the revision of the Data Protection Directive. Despite the modern nature of the DPD at the time of its adoption, almost 20 years have since passed, rendering it ill-suited to meet the needs and challenges of modern data processing. The wish to delete data about oneself online is no longer seen as an action borne out of a fear of governmental surveillance, but rather, an option that many consider to be vital for a healthy reputation and successful professional life.

Furthermore, the great derogations in data protection laws of Member States called for an update of the rules.[117] Despite its adoption in 1995, many States took six or seven years to announce their implementation measures, meaning that technological advances during these years provided a large obstacle to harmonization.[118] Additionally, as the DPD was not a maximum harmonization measure, but permitted Member States with pre-existing data protection laws with more extensive protection to subsist, the European Union has ended up with a fragmented data protection landscape.[119] The Commission found that this legal fragmentation of the European Union data protection framework hampered the outcome of the "internal market objective."[120] Having been adopted to benefit and

---

[112] *Id.*

[113] *Id.* para. 100.

[114] *Id.* paras. 35–38.

[115] *Id.* para. 100.

[116] *Id.* paras. 69, 71, 81.

[117] *See Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, at 2–3, 7, COM (2012) 9 final (Jan. 25, 2012).

[118] *See First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 3, 7, 10, COM (2003) 265 final (May 15, 2003).

[119] *See Private Data, Public Rules*, ECONOMIST, Jan. 28, 2012, http://www.economist.com/node/21543489.

[120] *Impact Assessment Accompanying 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*

promote the internal market, the DPD could thus not live up to its full economic potential.[121]

In 2012, the Commission adopted a proposal for reforming the data protection regime of the European Union entitled the General Data Protection Regulation (GDPR) that aims to incorporate the "right to be forgotten" and "the right to erasure."[122] The proposal attempts to empower data subjects by giving them the right to request that their personal data is fully removed when it is no longer needed for the purposes for which it was collected, therefore, enabling them to obtain a clean slate.[123]

One stated goal of the GDPR is protecting privacy retroactively. The proposal includes a specific reference to data made public while the data subject was a child. This is intended to highlight the importance of retrospective privacy—in the sense that people who become privacy-aware later in life should not be left without protection.[124]

Movement of such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data, at 11, SEC (2012) 72 final (Jan. 25, 2012).

[121] The nature of a Directive allows for a certain margin of discretion between Member States in their implementation of European Law. *Monitoring Implementation of EU Directives*, EUR. COMMISSION, http://ec.europa.eu/atwork/applying-eu-law/implementation-monitoring/index_en.htm (last updated Feb. 8, 2015). Conversely, a Regulation has horizontal direct effect and applies in the same manner to each Member States as written.

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

[123] *See* Council Directive 95/46, art. 2, 1995 O.J. (L 281) 31, 38 ("'[P]rocessing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."); *see also* Viviane Reding, Vice-President of the European Comm'n Responsible for Justice, Fundamental Rights and Citizenship, Speech at the American Chamber of Commerce to the EU: Building Trust in Europe's Online Single Market (June 22, 2010), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference-SPEECH/10/327.

[124] "This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet." GDPR 2012, *supra* note 122, at 25. The European Parliament's amended draft does not contain the reference to the right applying "specifically to [when the data subject was] a child." *See Resolution of 12 March 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) (Mar. 12, 2014) [hereinafter GDPR 2014], *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN. Such a removal brings a more linear right, as it effectively applies to all data subjects wishing to delete data about themselves and not only those who published data when they were children. Still, as will be shown below, the very inclusion of this wording indicates that, at the heart of the matter, the E.U. and U.S. approaches are more similar than they appear at first glance.

The amended draft of the GDPR was approved by the European Parliament following the vote in plenary on March 12, 2014.[125] The amended text does away with the highly controversial "right to be forgotten" label and replaces it with "the right to erasure."[126] While the name change may serve to lessen its contentious nature by aligning it with the current wording of the Data Protection Directive, a close reading of the amended text shows that the main elements of "the right to be forgotten" remain.[127]

The European Council is still debating the text and it is not clear what the final text after deliberation will look like. According to Article 17(1) of the proposed Regulation:

> The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data . . . where one of the following grounds applies:
>
> (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
>
> (c) the data subject objects to the processing of personal data pursuant to Article 19;
>
> (d) the processing of the data does not comply with this Regulation for other reasons.[128]

If the proposed amendments are adopted, the GDPR would retain the same exceptions as the DPD, including: areas falling outside the scope of Union law, such as national security,[129] information relating to the prevention, investigation, detection, or prosecution of criminal offences,[130] and the household exemption.[131] The GDPR would also explicitly set out that the "Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive."[132]

What Article 17 does offer is a clearer right to have data deleted. There is no longer a requirement for the data to be inaccurate or not in line with the legal

[125] GDPR 2014, *supra* note 122. It should, however, be noted that the majority of legislation following the co-decision procedure leaned towards the opinion of the Council.

[126] *Id.*

[127] *Id.*

[128] *Id.* art. 17(1), at 51.

[129] *Id.* art. 2(2)(a), at 40.

[130] *Id.* art. 2(2)(e), at 40.

[131] *Id.* art. 2(2)(d), at 40. This article has been amended to include language stating that the activity of the person must be "without any gainful interest in the course of its own exclusively personal or household activity." *Id.*

[132] *Id.* art. 2(3), at 41.

framework; the GDPR outlines that data must be deleted upon withdrawal of consent.[133] This alleviates the uncertainty of the DPD. Additionally, there is the novel requirement that the data should be deleted if the agreed time period for storage has expired. Such a time period might be achieved through the application of specific meta-data, which catalogues expiration values of data or through another form of technical solution.[134] The Regulation here relies heavily on technical privacy-by-design measures, which would allow controllers to attach a time frame (or expiration date) to data.

Finally, Article 17 includes an obligation for data controllers, who are responsible for the publication of data, to take all reasonable steps, including technical measures, "to inform third parties . . . that a data subject requests [erasure of personal data]."[135] Additionally, where there had been publication by a third party and "[w]here the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication."[136]

Ultimately, the right to be forgotten in Europe has a fundamental basis in primary law. This right is rooted in the enumerated protection of privacy found in both the ECHR and the European Charter of Fundamental Rights. The CJEU has further protected data subjects by finding that search engines, such as Google, have a legal obligation to sever links to material which no longer serves a fundamental purpose and for which the subject objects. And the European Union has implemented (and will soon implement) further processes to enable data subjects to exercise this right.

II. THE AMERICAN RIGHT TO BE FORGOTTEN

The right to privacy (and by extension, the "right to be forgotten") in the United States is a far more opaque right. It is un-enumerated and more controversial. Yet, there is a basis for such a right, although more tenuous and more difficult to find.

A. Basis for the Right: American Privacy

One might get the impression from discussions surrounding the CJEU's *Google Spain* decision that the Europeans are alone in their quest to be forgotten. However, there is an emerging right to be forgotten in the United States as well. A major restraint on its development has been the free speech protections found in the First Amendment. The following section will briefly examine where the right to privacy comes from in the United States. From there, the tension between

---

[133] *Id.* art. 2, at 40–41.

[134] Steven C. Bennett, *The "Right To Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 180–181 (2012).

[135] GDPR 2012, *supra* note 122, art. 17, at 51.

[136] *Id.*

personality rights and free speech will be explored. Finally, efforts underway in the U.S. to secure a right to be forgotten will be examined.

The legal basis for regulation in the United States is much more elusive when compared to the legal basis in the European context. While the rights of the Convention are equal, and should be balanced against each other, the competing rights enshrined in the Bill of Rights are not as easily balanced. The competing rights at stake when one speaks about the "right to be forgotten" are the non-enumerated right to privacy and the right of free expression protected by the First Amendment. Privacy is never expressly mentioned in the text of the U.S. Constitution or Bill of Rights; instead, it is often seen as a thread that continues throughout the entire document.[137] It is fundamentally a right against *governmental* intrusion, rather than private intrusion.[138] Its fingerprints can be seen in the First Amendment's protection of religion or conscience, as a protection against governmental intrusion into how one might choose to worship.[139] Similarly, it is reflected in the right of association, the prohibition against quartering soldiers and the prohibition against unreasonable search and seizure.[140] The idea of the right to privacy in the American context was first expressed in 1890 by the noted professors Warren and Brandies in their article *The Right to Privacy*, and it more closely resembles a right to be left alone rather than a right to privacy in the European sense.[141]

The constitutional jurisprudence regarding the development of constitutional privacy right, including *Griswold v. Connecticut* (1965),[142] *Eisenstadt v. Baird* (1972),[143] *Roe v. Wade* (1972),[144] and *Lawrence v. Texas* (2003),[145] all focus on the state's intrusion into the applicant's private decision-making process. Private or corporate action has not fallen under constitutional prohibition, rather private actions are addressed under a common law tort of *invasion of privacy*.[146] This cause of action protects individuals against nongovernmental intrusion of their privacy.[147] The problem with assertion of this right is that it is disparate amongst the states of the United States.[148] Many states do not recognize the tort of invasion of privacy.[149]

---

[137] *See* Griswold v. Connecticut, 381 U.S. 479, 483–85 (1965) (discussing several of the proverbial penumbras in the constitution where privacy is protected).

[138] *See id.* at 483–84 (stating that the right to privacy protections in the First, Fourth, and Fifth Amendments are from governmental intrusion); *see also* Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (stating generally that the right to privacy is "the right of the individual . . . to be free from unwarranted governmental intrusion").

[139] *See Griswold*, 381 U.S. at 483.

[140] *See id.* at 483–84.

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

[142] 381 U.S. at 480, 485–86.

[143] 405 U.S. at 440–41, 453.

[144] 410 U.S. 113, 153 (1973).

[145] 539 U.S. 558, 577–79 (2003).

[146] *See* Warren & Brandeis, *supra* note 141, at 211, 218–19.

[147] *Id.*

[148] *See* MARY MCTHOMAS, THE DUAL SYSTEM OF PRIVACY RIGHTS IN THE UNITED STATES 21 (Robert M. Howard ed., 2013).

Scholars such as William Prosser, Anita Allen, and Mary McThomas have struggled to identify the basis for privacy protection in the American system. McThomas, synthesising theorists before her, has identified two strains that are relevant to a discussion of the "right to be forgotten."[150] The first is *decisional privacy*, and the second being *proprietary privacy*. [151] Decisional privacy encompasses grand rights of self-determination and liberty, some of which include the right to marry in all of its forms, reproductive freedom, and other autonomy-based rights.[152] Proprietary privacy rights are those that concern ones image, both in a real sense (e.g., photographs, etc.) and a less concrete way, such as reputation.[153] These rights, rather than being based upon autonomy or liberty theories, are rooted in a *protection of property rights* analysis.[154] McThomas asserts that courts (and legislatures) are more likely to protect proprietary privacy rights as opposed to decisional rights, perhaps because they are in some way more tangible and are perceived as much more singular.[155] A decision on whether same-sex marriage should be allowed for one set of litigants has great societal impact, whereas the award of damages for the violation of a duty to protect private data may not seem to have similar import.

Since proprietary privacy rights are rooted in a concept of ownership, a key issue regarding the "right to be forgotten" in the United States centers around ownership of the information in question. Whereas there is a great acceptance in Europe that one's reputation belongs to oneself, this concept is not as widely accepted in the United States.[156] If the data in question belongs to the individual, rather than the Internet platform, there is a greater likelihood that courts would be willing to enforce the individual's right to control this data.[157]

The counter-posed right is that of the freedom of the press: "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."[158]

While today this right is viewed by many as fundamental to the very fabric of American democracy, it was not litigated to any measure until after the First World War.[159] Slowly, the U.S. Supreme Court began to protect more and more facets of speech, but most important of all was the freedom of political speech and the freedom of the press.[160] Competing with this right—particularly coming out of the common law system—was tort, and sometimes the crime of defamation, in which

---

[149] *See id.*
[150] *Id.* at 2–4.
[151] *Id.*
[152] *Id.* at 3.
[153] *Id.* at 3–5.
[154] *Id.*
[155] *Id.* at 5–7.
[156] *See id.* at 23.
[157] *See id.*
[158] U.S. CONST. amend. I.
[159] *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 299 & n.3 (1964) (Goldberg, J., concurring).
[160] *See id.* at 270–71 (Brennen, J.).

litigants were given a cause of action for injury to reputation at the hands of an individual or newspaper.[161]

In 1964, the Supreme Court greatly changed the playing field by constitutionalizing the analysis of defamation, specifically the law of libel or written defamation.[162] In *New York Times Co. v. Sullivan*, the Court held that in defamation cases involving public officials, the plaintiff must prove that not only was the statement false, but also that the publisher acted with *actual malice*, indicating that the publisher either intended to publish the false statement, or that she acted with *reckless disregard* for the truth or falsity of the statement. At its core was a prioritization of speech and public debate over privacy and reputation.[163]

In *Curtis Publishing Co. v. Butts*, the Court extended the analysis to private individuals, finding that the defamation analysis differs in the context of non-public figures.[164] In this case, the Court held that a defamation claim does not require proof only of actual malice.[165] If the false published statement is merely recklessly collected or disseminated, the cause of action for defamation will be sustained.[166]

The shared principle between *New York Times* and *Curtis Publishing*, however, is that truth trumps privacy. If the statement is true, no matter how damaging, no matter if the subject is a public or private person, the claim cannot succeed.

B. American Efforts to be Forgotten

Given the emphasis on priority of speech over privacy, the idea of a "right to be forgotten" may seem very foreign to the American culture. It is not that there is a particular *right to remember*—yet the role of the press is just that. What has changed are the tools by which the press (and thereby the public) are able to remember. This poses no problem when specifically dealing with public officials. While the European context does not specifically differentiate between public and private individuals in defamation law, the courts often look at the value of the information to the public discourse.[167] Presumably, some information, particularly when it comes to issues of public concern, is relevant long after its collection or publication, regardless of its damage to reputation. More difficult are the cases involving the collection, use, and potential publication of data that are of very limited worth to a grander public discussion. In these cases, the American system might be willing to venture into the waters of greater privacy protection, particularly because of the limited impact upon the freedom of expression.

---

[161] *See id.* at 301–02 & n.4 (Goldberg, J., concurring).
[162] *See id.* at 301–02.
[163] *Id.* at 279–80 (Brennen, J.).
[164] Curtis Publ'g Co. v. Butts, 388 U.S. 130, 154–55 (1967).
[165] *Id.* at 164–165.
[166] *Id.*
[167] *See generally* Von Hannover v. Germany (No. 2), 2004 Eur. Ct. H.R. 294.

With respect to data of individuals that is collected by Internet services, rather than public information reported in the press, the regulation of that data and the individual's control over it is not very clear. Rather than an overarching legal strategy, legislation has focused on certain isolated realms of data. For instance, the privacy of health care data is protected by the Health Insurance Portability and Accountability Act (HIPAA), which requires that holders of private health care information not disclose information to third parties without the authorization of the data subject.[168] There are also provisions that guard against disclosure of financial information without authorization in specific cases. However, these mechanisms are geared more towards preventing discrimination against the data subject rather than protecting a sacred right. There does seem, however, to be an Internet privacy movement beginning in the U.S. In the wake of the National Security Agency (NSA) surveillance disclosures, the American think tank, The Pew Foundation found that American Internet users are changing their browsing habits.[169] A report issued in September of 2013 found that 86% of users had taken steps to mask their identity while surfing the web.[170] Furthermore, 41% had attempted to delete or edit past posts, while 55% had taken steps to avoid surveillance by certain people, organizations or governmental entities.[171] Interestingly, 68% of users believed that laws to protect online privacy in the United States were inadequate.[172] This and similar sentiments may be behind modest efforts in the U.S. to provide some form of protection for the most vulnerable Internet users.

Two legislative efforts currently underway in the United States exemplify the American perspective on data protection privacy. The first is California Senate Bill 568, a measure that went into force on January 1, 2015.[173] The second is a proposed federal legislation entitled Do Not Track Kids Act of 2013, which is currently making its way through the Congress.[174] Both the California law and the Federal proposal can be seen as preliminary steps in limiting the availability of information. This limitation may have social value on a macro scale; however, it might also have great consequences on individuals. Both measures are also part of a greater effort to protect children in a cyber environment.

---

[168] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1177, 10 Stat. 1936, 2029.

[169] *See* LEE RAINIE ET. AL, PEW RESEARCH CENTER, ANONYMITY, PRIVACY, AND SECURITY ONLINE 2 (2013), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf.

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] S. 568, 2013 Leg., Reg. Sess. (Cal. 2015).

[174] Do Not Track Kids Act of 2013, S. 1700, 113th Cong. (2013). Previous legislative attempts had been undertaken in 2011 with the Do Not Track Kids Act of 2011. *See* Press Release, Ed Markey, U.S. Senator for Mass., May 13, 2011: Markey, Barton Introduce Bipartisan 'Do Not Track Kids Act' (May 13, 2011), *available at* http://www.markey.senate.gov/news/press-releases/may-13-2011-markey-barton-introduce-bipartisan-do-not-track-kids-act.

1. California Senate Bill 568's Limited Right to be Forgotten.—In September 2013, California Governor Jerry Brown signed into law a measure amending the California Business and Professions Code, relating to the internet. [175] The amendment, California Senate Bill 568 ("The Act"), seeks to give some users of social media a right to erasure.[176] The Act, which went into effect in January of 2015, is limited in scope and in application. It has been derided as an unconstitutional intrusion on the right of free speech, and as a mechanism that is too narrow to actually protect its stated interests.[177]

The adopted Act is remarkably simple in its approach and limited in its application. It does not protect a general "right to be forgotten" as it only protects minors from materials which they have posted online themselves.[178] Additionally, the legislation's aims are coupled with other concerns regarding the use of the internet by vulnerable youths. The legislation requires that providers of web sites, online services, Internet applications, and mobile applications refrain from marketing or advertising specific types of products or services to minors.[179] The Act also prohibits these providers from knowingly using, disclosing, or compiling minor's personal information for purposes of advertising or marketing said products or services.[180]

Additionally, The Act requires operators to allow minors to remove content or information posted on the operator's website by the minor.[181] The law does not compel the operator to remove material if it is posted by a third person, if the operator is required to keep the information pursuant to federal or state law, or if the operator anonymizes the information.[182] Lastly, the operator is required to notify the users of their rights to removal pursuant to The Act.[183]

In enacting California Senate Bill 568, the legislature recognized that the balance between the rights of Internet users to privacy and the right to freedom of expression were out of sync in terms of social media used by young people. Especially given the prevalent usage of social media by minors, as well as the lack of

---

[175] Brett Lockwood & Katharine F. Rowe, *Client Alerts: New California Law Extends Additional Protection to Minors on the Internet,* SMITH, GAMBRELL, & RUSSELL, LLP (May 4, 2014), http://www.sgrlaw.com/resources/client_alerts/new-california-law-extends-additional-protections-to-minors-on-the-internet.

[176] Cal. S. 568.

[177] *See* Eric Goldman, *California's Latest Effort to 'Protect Kids Online' Is Misguided and Unconstitutional,* FORBES (Sept. 30, 2013, 11:50 AM), http://www.forbes.com/sites/ericgoldman/2013/09/30/californias-latest-effort-to-protect-kids-online-is-misguided-and-unconstitutional/.

[178] *See generally id.* (discussing the privacy interests of minors on the internet).

[179] *Id.* § 22580(i). This section identifies the products prohibited from online advertising or marketing to minors: alcoholic beverages, firearms, BB guns, handgun safety certificates, spray paint, etching cream that is capable of defacing property, tobacco products and paraphernalia, dangerous fireworks, tanning in an ultraviolet tanning devices, dietary supplements products containing ephedrine, lottery games, or products containing Salvia divinorum (a psycho-active plant). *Id.*

[180] *Id.* § 22580(c).

[181] *Id.* § 22581(a)(1).

[182] *Id.* § 22581(a)(2).

[183] *Id.* § 22581(b).

understanding of the effects of posting sensitive information on the internet, the legislature saw a need to protect children from themselves.

The effectiveness of the measure's erasure mechanism is questionable. It is limited in scope given that the wording of the provision only seems to cover individuals who post material *and* request its removal before they turn eighteen. While this provision might be interpreted as more expansive, allowing for the removal of posts made by individuals younger than eighteen by individuals over eighteen, this reading would seem to run contrary to the measure's plain wording. As far as the economic impact of the measure, there has been a deafening silence. Perhaps because of the duplicative nature of the measure, there has not been an outrage regarding this aspect of the legislation. There have, however, been grave doubts as to the constitutionality of the erasure requirement.[184]

A further complication occurs when a data subject wishes to delete personal information that has been provided by a third party. Many social networking sites, for example, retain the power to remove information that is deemed to be offensive or defamatory;[185] however, these sites often argue that issues relating to data posted by one user and not wanted by the other need to be sorted out personally between the two users.[186] This general policy leaves open the question: What happens when a picture is posted by an unknown person of the data subject or posted by a person with actual intent to cause damage to the data subject?

The Act implemented in California is quite clear in this situation. Only information submitted by the data subject can be removed and information posted by another individual is strictly off-limits—at least, if relying on these provisions.[187]

This issue is especially relevant in light of a recent Fourth Circuit Court of Appeals decision where the court held that there is First Amendment protection for "liked" material on Facebook, holding that "liking" something constitutes expression, which is protected.[188] This holding begs the question of whether deletion of material that has been "liked" then violates the "liker's" free speech interests. Furthermore, what if a third party user makes a comment on a post that might later be erased pursuant to the new law? When a social network devises its

---

[184] *See, e.g.*, Thomas R. Burke et al., *California's "Online Eraser" Law for Minors to Take Effect Jan. 1, 2015*, DAVIS WRIGHT TREMAINE LLP (Nov. 17, 2014), http://www.dwt.com/Californias-Online-Eraser-Law-for-Minors-to-Take-Effect-Jan-1-2015-11-17-2014/.

[185] *See, e.g.*, *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last updated Nov. 15, 2013) (stating that Facebook retains the right to "remove any content or information . . . post[ed] on Facebook if [it] believe[s] that it violates [the] Statement or [its] policies").

[186] *See, e.g.*, Larry Magid, *Facebook Builds Reporting Tools to Encourage 'Compassion,'* HUFFINGTON POST (July 19, 2012, 7:23 PM), http://www.huffingtonpost.com/larry-magid/facebook-builds-reporting_b_1686464.html (noting that Facebook is "experimenting with 'social reporting' designed to encourage users to work out issues between themselves . . .").

[187] *See* Cal. S. 568 § 22581. Admittedly, this is done in an attempt to ensure that the right to freedom of expression is not infringed upon.

[188] *See* Bland v. Roberts, 730 F.3d 368, 386 (4th Cir. 2013); *see also* Joe Palazzolo, *Court: Facebook 'Like' Is Protected By the First Amendment*, WALL ST. J. (Sept. 18, 2013, 9:55AM), http://blogs.wsj.com/law/2013/09/18/court-facebook-like-is-protected-by-the-first-amendment.

own policies that outline erasure, there is no governmental interference with the freedom of speech right, which might trigger the application of the First Amendment. However, when the erasure is mandated by statute, the state action is more apparent.

2. Do Not Track Kids Act of 2013.—Fitting hand-in-glove with the California legislation is a federal effort to extend the California protection to the rest of the United States. In 2011, then Representative Edward Markey proposed amendments to the Children's Online Privacy Protection Act of 1998 to extend a "right to be forgotten" to children.[189] While this bill was never adopted, Edward Markey—this time a senator—proposed a similar bill in 2013.[190] The new amendments contained in the Do Not Track Kids Act of 2013 require use of a delete button, whereby children have the ability to delete material hastily posted.[191] Representative Markey saw this right as one that should be extended to all online users, but argued that the protection of children was a good starting point.[192] Similar to the California measure, the Do Not Track Kids Act requires websites to inform users of what information is being collected and for what purpose.[193] The law requires that websites obtain permission from the parents of minor users before data is collected.[194] The legislation also prohibits the use of the material for marketing purposes.[195] Lastly, the law requires the erasure button described above.[196] Once prompted, the extent of the duty to erase material is simply to make the material unavailable to third parties.

The original Children's Online Privacy Protection Act (the precursor to the Do Not Track Kids Act) came into force in 1998 and prohibited the collection of "personal information" of children under thirteen years of age without the "verifiable consent" of a parent.[197] The Act empowered the Federal Trade Commission (FTC) to promulgate regulations to implement these protections.[198] In 2000, the FTC promulgated the original rule, which defined "personal information" as little more than the name, address, telephone number, social security number, and birthdate of the child.[199] Due to changes in technology, the FTC broadened the scope of the definition of "personal information" in 2013 to

[189] Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011) (amending the Children's Online Privacy Protection Act of 1998 to apply the prohibitions against collecting personal information from children to online applications and mobile applications directed to children).

[190] Christin S. McMeley, Paul Glist & Leslie Gallagher Moylan, *Federal Lawmakers Revive Do Not Track Kids Legislation,* DAVIS WRIGHT TREMAINE LLP (Nov. 18, 2013), http://www.dwt.com/Federal-Lawmakers-Revive-Do-Not-Track-Kids-Legislation.

[191] *See* Do Not Track Kids Act of 2013, S. 1700, 113th Cong. § 7(b)(1)(A) (2013).

[192] Ambrose & Ausloos, *supra* note 65, at 14.

[193] *See* S. 1700 § 3.

[194] *See id.*

[195] *See* S. 1700 § 4.

[196] *See id.* § 7(b)(1)(A).

[197] 15 U.S.C. §§ 6501, 6502(a),(b) (2012).

[198] *Id.* § 6505.

[199] 16 C.F.R. § 312.2 (2000) (defining personal information).

include user names and geo-locations—which identify a child's location, photographs, and voice files.[200]

The proposed amendments also expand coverage of the Do Not Track Kids Act to minors between thirteen years old and fifteen years old, potentially significantly altering compliance requirements for companies such as Facebook, which only accepts clients older than thirteen years old.[201]

What these measures reflect is a priority to protect the personality interests of the most vulnerable. Whereas Senator Markey sees future action to extend the protections to adult Internet users, the realization of this goal seems far off into the future, if feasible at all. The non-profit, government transparency watchdog group, GovTrack, which monitors proposed Congressional legislation, gives the measure only a two percent chance of being enacted in the current session, despite bipartisan support in both houses of Congress.[202] Notwithstanding this prognosis, legislatures are more willing to sponsor measures that protect against the dangers of the Internet's memory, representing a possible shift in the debate.[203] Because these protective measures are extremely far-reaching, not only they can surely assuage concerns regarding the privacy of minors, but they can protect against certain Internet abuses as well.

3. Revenge Porn.—One area where the "right to be forgotten" would prove fortuitous is for revenge porn sites. Revenge porn sites post intimate, unauthorized photos of celebrities, jilted lovers, and those wishing to embarrass or harass sexual partners.[204] Revenge porn can have devastating effects on its victims, and there is a certain justice at stake that might not be as evident as with the right of eraser. Often the images are not only unauthorized, but are also obtained illegally by hacking. In the European Union, especially in light of the *Google Spain* decision, victims are able to have the images suppressed by cutting the link to them within searches.[205] Conversely, the United States has struggled with how to protect those who are directly affected. The infamous U.S. example of Hunter Moore, proud

---

[200] 16 C.F.R. § 312.2 (2014) (redefining personal information to reflect technological changes).

[201] *Id.*; *see also* Emam Llansó, *Do Not Track Kids Bill Revives Minors' Online Privacy Debate*, CTR. FOR DEMOCRACY & TECH. (Nov. 26, 2013), https://cdt.org/blog/do-not-track-kids-bill-revives-minors'-online-privacy-debate/; *Statement of Rights and Responsibilities,* FACEBOOK, https://www.facebook.com/legal/terms (last updated Nov. 15, 2013) ("You will not use Facebook if you are under 13.").

[202] *S. 1700 (113th): Do Not Track Kids Act of 2013*, GOVTRACK, https://www.govtrack.us.congress/bills/113/s1700 (last visited Feb. 8, 2015).

[203] *See* Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, NY TIMES (Oct. 30, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?pagewanted=all&_r=0.

[204] *See* Ave Mince-Didier, *Revenge Porn: Laws & Penalties,* CRIMINAL DEF. LAWYER, http://www.criminaldefenselawyer.com/resources/revenge-porn-laws-penalties.htm (last visited Feb. 8, 2015).

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

former proprietor of a revenge porn blog,[206] illustrates this point. Through his site entitled "Is Anyone Up?," Moore hosted a platform where users could post such intimate pictures.[207] On his site, Moore encouraged the posts and benefited from advertising revenue generated from the images. [208]

Moore relied on Section 230 of the Communications Decency Act of 1996 for protection from liability for the content of his website, arguing that he was acting merely as a hosting provider, and that the data controllers would be the individuals actually uploading the pictures and information within them, and thus the parties responsible in terms of liability.[209] Yet, if Moore were in the European Union, the analysis would be somewhat different. Because Moore gained commercial benefit from the website, exercised editorial control over it, and organized the content, he might rise to the level of "controller" and would thus fall within the scope of the GDPR.[210]

As public pressure mounted and the FBI began an investigation of Moore for paying hackers to obtain photos that appeared on his site, Moore sold his enterprise to an anti-bullying site named bullyville.com.[211] In January of 2014, Moore and a co-defendant Charles "Gary" Evens, were charged with fifteen counts of violations of unauthorized access to a protected computer (also known as hacking), aggravated identity theft, conspiracy, and aiding and abetting.[212] The trial in these matters has been postponed until 2015.[213]

---

[206] *See* Jessica Roy, *Revenge Porn King Hunter Moore Was Arrested, But Not for Hosting Revenge Porn*, TIME (Jan. 27, 2014), http://newsfeed.time.com/2014/01/27/revenge-porn-king-hunter-moore-was-arrested-but-not-for-hosting-revenge-porn.

[207] *See* Emily Greenhouse, *The Downfall of the Most Hated Man on the Internet*, THE NEW YORKER (Jan. 28, 2014), http://www.newyorker.com/tech/elements/the-downfall-of-the-most-hated-man-on-the-internet.

[208] *See id.*

[209] *See* Roy, *supra* note 206. *But see* Delfi AS v. Estonia, Eur. Ct. H.R. App. No. 64569/09 (2013), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635. In this European Court of Human Rights case, a news outlet was held responsible for anonymous defamatory comments submitted to the news outlet's website. *See id.* para. 94, at 32. The national court held the news outlet responsible for the comments with the latter appealing to the ECHR arguing that their Article 10 right to freedom of expression had been infringed and that, subject to Article 14 of the E-Commerce Directive, they could not be held liable. *See id.* paras. 46, 52, 53 at 18–20. The ECHR stated that there was no infringement because the news outlet should have anticipated the onslaught of comments and reacted accordingly. *See id.* para. 86, at 29. Furthermore, as the commenters were anonymous and would be highly difficult to find, holding the news outlet liable was reasonable, especially as it drew commercial benefit from the comments. *See id.* para. 94, at 32.

[210] GDPR 2012, *supra* note 122, art. 4, at 41 (defining "controller" as the "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data").

[211] *See* Camille Dodero, *"Gary Jones" Wants Your Nudes*, THE VILLAGE VOICE, (May 16, 2012), http://www.villagevoice.com/2012-05-16/news/hacker-is-anyone-up-hunter-moore-fbi/.

[212] *See* Indictment, United States v. Moore, No. 13-0917 (C.D. Cal. Dec. 20, 2013), *available at* http://ia600507.us.archive.org/4/items/gov.uscourts.cacd.579295/gov.uscourts.cacd.579295.1.0.pdf (listing the charges against the defendants for violation of unauthorized access to a protected computer, aggravated identity theft, conspiracy, and aiding and abetting).

[213] Order Continuing Trial Date and Findings Regarding Excludable Time Periods Pursuant to Speedy Trial Act, United States v. Moore, No. 13-0917 (C.D. Cal. Nov. 4, 2014).

The Moore case follows the 2012 conviction of Christopher Chaney, a hacker who posted photos of celebrities and non-celebrities alike.[214] He received a sentence of ten years in federal prison after pleading guilty to charges including wiretapping and unauthorized access to a computer.[215] Chaney particularly targeted female celebrities.[216] Many of the photos he posted appear to still be available on different sites on the internet. In both the Moore and Chaney cases, prosecutors targeted the hacking rather than the image posting to obtain convictions. The deficiencies in existing data protection law are shown by the fact that the images remain with no effective remedy for removal.

Against this backdrop, several states have introduced measures that criminalize the act of posting these private images with the intent to humiliate their subjects. One such measure amends the Disorderly Conduct section of the California Penal Code and holds liable:

> Any person who photographs or records by any means the image of the intimate body part or parts of another identifiable person, under circumstances where the parties agree or understand that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious emotional distress, and the depicted person suffers serious emotional distress.[217]

Additional efforts to eradicate revenge porn will perhaps prove more effective. In December of 2013, California Department of Justice agents arrested a revenge porn operator, Kevin Bollaert, for allegedly posting sexualized images of unwilling subjects, on charges of conspiracy, identity theft, and extortion.[218] California's Penal Code makes it illegal to "willfully obtain someone's personal identifying information, including name, age and address, for any unlawful purpose, including with the intent to annoy or harass."[219] In violation of this statute, Bollaert, the operator of ugotposted.com, posted more than 10,000 nude photos of unwilling subjects.[220] However, Bollaert was not charged under the new California law, but rather under identity theft and extortion provisions of federal law, as he identified

---

[214] *See Christopher Chaney, So-Called Hollywood Hacker, Gets 10 Years for Posting Celebrities' Personal Photos Online*, CBS NEWS (Dec. 18, 2012, 10:02 AM), http://www.cbsnews.com/news/christopher-chaney-so-called-hollywood-hacker-gets-10-years-for-posting-celebrities-personal-photos-online/.

[215] *Id.*

[216] *See id.*

[217] CAL. PENAL CODE § 647(j)(4)(A) (West 2014).

[218] *See* Don Thompson, *Court Date Set for Kevin Bollaert in Revenge Porn Website Case*, HUFFINGTON POST (Jan. 23, 2014, 1:38 AM), http://www.huffingtonpost.com/2013/12/12/kevin-bollaert-revenge-porn_n_4432097.html.

[219] Press Release, Kamala D. Harris, Att'y Gen., Cal. Dep't of Justice, Attorney General Kamala D. Harris Announces Arrest of Revenge Porn Website Operator (Dec. 10, 2013), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-arrest-revenge-porn-website-operator; *see also* CAL. PENAL CODE §§ 530.5, 653m(b) (West 2014).

[220] *See* Press Release, Kamala D. Harris, *supra* note 219.

the victims and extorted them by offering to remove the images for a fee between $250 and $350.[221]

Importantly, the provisions of California's new legislation do not require removal of the material; rather, the poster of the material is liable for a misdemeanor.[222] Consequently, a user who posts a sexual "selfie," which he later regrets, has no recourse for removing or forgetting the image.[223] However, the provisions taken together seek to give vulnerable members of society control over the way they are represented. Yet this protection, like the protection envisioned in the European Union General Data Protection Regulation, is limited in what images can be erased. If third parties post these images and are justified in doing so, the subject will not be successful in their attempt to have the material erased. Yet if the images are of a sexual nature and were intended for personal and intimate consumption, then the subject might have redress.[224]

III. FORGETTING: AN EFFECTIVENESS MEASURE – OR, THE CRUMBLY ERASER?

The questions that are left after the exploration of what extent the "right to be forgotten" exists in Europe and the United States are that of necessity and implementation.

Acknowledging that in Europe, there exists a basis for the right in primary law, and in the United States a much more limited, exception basis, an important question that remains is whether the "right to be forgotten" is worth all the hype? Given that "the right to be forgotten" arguably impinges upon the freedom of expression, and could potentially cost search engines and other web-based businesses millions, is it effective?[225]

On the question of necessity, a further understanding of what remains on the internet is essential. Legal scholar Meg Ambose asserts that ephemerality is a key concept of the Internet. She posits that most information posted on the Internet is subsumed by its vastness within a couple of months.[226] Additionally, rather than an organized library of information, the internet more closely resembles a warehouse of poorly categorized material. Called by some the world's largest Xerox

---

[221] *See* Thompson, *supra* note 218.

[222] CAL. PENAL CODE § 647(1) (West 2014).

[223] Eric Goldman, *California's New Law Shows It's Not Easy to Regulate Revenge Porn*, FORBES (Oct. 8, 2013, 12:03 PM), http://www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn/.

[224] CAL. PENAL CODE, *supra* note 217.

[225] *See* Craig A. Newman, *'A Right To Be Forgotten' Will Cost Europe*, WASH. POST (May 26, 2014), http://www.washingtonpost.com/opinions/a-right-to-be-forgotten-will-cost-europe/2014/05/26/93bb0e8c-e131-11e3-9743-bb9b59cde7b9_story.html (noting that the costs of the right to be forgotten likely will be astronomically high, yet truly incalculable, due to the potential of millions of deletion requests and removal demands).

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

machine,[227] the internet is made up of a series of images that are not readily associated or categorized. Ambrose, among others, has argued that the perception that information held on the internet is permanent is a misconception.[228] She asserts that Internet information is particularly susceptible to degradation, primarily from technical conditions that require individual sites to be maintained as time passes.[229] Additionally, as sites are preserved and updated, information that might be the target of an asserted "right to be forgotten" is lost as individual pages are changed. In her article on the ephemeral nature of such information, Ambrose cites studies which found that ninety per cent of information was changed (and therefore was lost) over a period of ten days.[230] Yet these same studies indicate that it takes nearly eight and a half years for the selected sample of URLs to change completely.[231] Additionally, as potentially embarrassing information ages, its "rank" within the search engine index falls since its availability is directly tied to the amount of hits it receives. Ironically, the information becomes less accessible (lower on the rank of search results) the less searchers that click on the link, and less searchers then click on the link as the material becomes less retrievable. This self-eating snake scenario minimizes the need for a strict "right to be forgotten."

Information is more secure and durable in maintained archive systems, such as those preserved online by newspapers. This was the circumstance in *Google Spain*, where particular information held in a newspaper article was the subject of Mr. Costeja-Gonzalez's complaint.[232] Interestingly, the CJEU did not find that the material on the original new site ought to be removed, but rather Google had a responsibility to cut the link between the search and the information.[233] The archive is then left intact on the internet; however, retrieving the information is more difficult.

A second and perhaps more worrying question concerns how the right to be forgotten, particularly after the *Google Spain* decision, will be implemented? In this regard, it is important to remember that since search engines are not *publishers* of the original material, their free speech interests might be less than the original author or publisher. As search engines attempt to limit their litigation costs, including exposure to damages, which might be incurred under the new regulation,

---

[227] Hamilton Nolan, *The Internet Is the Biggest Threat to Publishing Since the . . . Xerox Machine?*, GAWKER (Mar. 13, 2012, 11:02 AM), http://gawker.com/5892819/the-internet-is-the-biggest-threat-to-publishing-since-the-xerox-machine (quoting John R. "Rick" MacArthur, Harper's Magazine Publisher) (stating that the internet is just a huge Xerox photocopier with an "inhuman memory").

[228] *Id.*; *see also* Paulan Korenhof et al., Timing the Right To Be Forgotten: A Study into "Time" as a Factor in Deciding about Retention or Erasure of Data (May 13, 2014) (unpublished paper), *available at* http://ssrn.com/abstract=2436436.

[229] Ambrose, *supra* note 226.

[230] *Id.* at 392.

[231] *Id.*

[232] Case C-131/12, Google Spain SL Google, Inc. v. Agencia Española de Protección de Datos (AEPD) (E.C.J. May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang-EN &docid=152065.

[233] *See id.*

some engines will prefer to err on the side of caution rather than risk fines for keeping links to materials in the interest of the public. This seems to have already occurred. According to several reports, European Google outlets have severed links to past articles regarding poor decisions made by prominent business figures rather than risk exposure resulting from litigation.[234] Case and point, since the *Google Spain* decision, Google has received thousands of forget requests[235] and has severed one *BBC* report and six articles which appeared in *The Guardian* regarding the former CEO of Merrill Lynch.[236] The news items, which appeared in the mid 2000's, dealt with Stan O'Neal's departure from the ailing enterprise. It does not appear that there were inaccuracies in the articles, but rather they carried the potential to impact the former CEO's future job prospects. However, the collapse of Merrill Lynch was closely linked to an economic crisis, and the stories would qualify under an exemption for information valuable to the public interest. Yet, if a search engine doesn't want to incur the costs of litigation against a well-heeled opponent, it makes more business sense to simply honor the request to delete the information. Neither the BBC nor The Guardian would have standing to challenge Google – it would be Google's decision to make.[237] When voluntarily severed, there is no governmental oversight. The potential free speech implications in such cases are significant, and ultimately the credibility of the search engine might be called into question.[238]

When Google takes something down as a result of a "forget request," the company notifies searchers with a tag at the bottom of the search request, which states: "Some request may have been removed under data protection law in Europe. Learn more."[239] While it may be that Google is acting with understandable caution, it may also be trying to show the impact of the *Google Spain* ruling on the availability of information after the ruling. Additionally, there is a question as to whether the notice which is posted after a removal will become worse than the material itself—searchers will be left to surmise what information was so horrible that it warranted removal. Inevitably, these issues will need to be addressed in 2015, when the European Union begins to craft the new Regulation. Perhaps there should be governmental (at least judicial) oversight of "forget requests" which would ensure that basic principles, such as the freedom of expression and the freedom to receive information are respected.

---

[234] *See* Paul Bernal, *Is Google Undermining the 'Right To Be Forgotten'?*, CNN (July 7, 2014), http://edition.cnn.com/2014/07/07/opinion/bernal-google-undermining-privacy-ruling/.

[235] *See* Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion.

[236] *See* Jim Edwards, *Google Is Being Forced To Censor the History of Merrill Lynch — And That Should Terrify You*, BUS. INSIDER (July 3, 2014, 6:48 AM), http://www.businessinsider.com/google-merrill-lynch-and-the-right-to-be-forgotten-2014-7.

[237] Robert Peston, *Why Has Google Cast Me into Oblivion?*, BBC NEWS (July 2, 2014), http://www.bbc.com/news/business-28130581.

[238] *See* Edwards, *supra* note 236; *see also* James Ball, *EU's Right To Be Forgotten: Guardian Articles Have Been Hidden by Google*, THE GUARDIAN (July 2, 2014), http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google.

[239] Edwards, *supra* note 236.

In response to the *Google Spain* decision, legislative initiatives, and perhaps consumer agitation, online providers have begun to take action to ameliorate the feeling that individuals are not in control of their online profiles. The most notable of these initiatives is the voluntary "erase" buttons and policies for erasure offered by such websites as Facebook. In theory, these services offer users the opportunity to delete information from their profiles, yet the question remains as to whether this merely hides the information or truly deletes it. Assuming that the information is simply not accessible, is this move sufficient to stave off calls for legislative measures? Additionally, will this information still be available to companies for purposes of marketing or to law enforcement and security officials for investigatory purposes?

Other platforms, such as the one employed by the app "SnapChat," employ a time limitation for the availability of information, whereby a message—in the case of SnapChat a video message—is only available for a short period of time, after which it disappears. These messages, however, can be captured on the recipient's device and thereby preserved and possibly re-disseminated.[240] The promise of this fleeting nature of communication however is not so clear as SnapChat recently settled a complaint with the United States Federal Trade Commission for deceptive practices regarding the service's promised deletion.[241] Yet, the idea or desirability of this feature remains popular among users. Currently, Facebook is also exploring a similar service.[242] While this type of ephemerality may satisfy some privacy advocates, law enforcement officials might find it particularly troublesome—the inaccessibility of information might be the equivalent of destruction of evidence in some cases where the platform is used for illicit purposes.

The measures mentioned above may have dual purposes. First, they may simply be a response to market conditions whereby privacy has become an attractive commodity. Alternatively, they may be an attempt to make legislative actions irrelevant—why are governmental protective measures needed if the industry has responded to protect consumers voluntarily? Or perhaps it is an attempt to repair the damage that the NSA scandal had on the reputation of Internet platforms. In light of recent revelations surrounding the NSA surveillance program that exposed the Federal Government's collection of Internet information and the service provider acquiescence to this collection, many technology firms are in the cyber hot

---

[240] When the image is captured by a recipient, the sender receives a message to this effect. *See Privacy Policy*, SNAPCHAT, https://www.snapchat.com/privacy (last updated Nov. 17, 2014) ("[U]sers who see your messages can always save them, either by taking a screenshot or by using some other image-capture technology . . . . If we're able to detect that a recipient took a screenshot of a message you sent, we'll try to notify you.").

[241] *See* Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[242] *See* Alexis Kleinman, *Facebook Is Testing Self-Destructing Posts*, HUFFINGTON POST (Sept.10, 2014, 2:59 PM), http://www.huffingtonpost.com/2014/09/10/facebook-self-destruct_n_5798320.html.

seat.[243] As users have become increasingly suspicious of technology firms, big providers have begun to seek ways to rebuild trust with their clients and the public as a whole.[244] To this end Microsoft and Google have sought to not only distance themselves from the actions of the United States federal agencies, and any acquiescence they may be guilty of, each have rolled out new privacy products since Edward Snowden's revelations in the summer of 2013. Adoption of a limited "right to be forgotten" might be a cost effective way of renewing trust with users and customers.

CONCLUSION

Today's interconnected world makes my private business, very much everyone's business. The internet never forgets, but maybe it should.

One of the major issues about the "right to be forgotten" is the fear that it could result in a Dark Age of the internet, where information mysteriously disappears and the past is deleted with a click of the mouse. Parties both in the United States and in the European Union worry that such a right could be used for, or result in, censorship. For example, the inability to maintain a successful public record for historical purposes, or the ability of one data subject to control their information infringing on the rights of another, such as the case of a data subject wanting to delete the information posted by a third party. It is the classic story of a clash of both principles and perspectives. An essential fundamental right to have access to and the ability to impart information is thrown against the rights of privacy, autonomy, and in some cases, dignity.

As the theoretical basis of privacy has grown up very differently in the United States and Europe, it is of little surprise that the conceptualization of a "right to be forgotten" also differs greatly. The conundrum was born in an era when time healed all wounds and individuals with a checkered past could cross an ocean or a prairie to start a new life. Individuals who are wrongly accused or the victim of horrible circumstances, who have made horrible mistakes or just had bad luck, have often sought refuge in a new town with a fresh start, but they have always run the risk that an old familiar face would appear in town to expose them as the fraud they are, or perhaps were. It is this tug of war between the value of memory and the ability to start anew, that is the question. In legal terms this competition is reflected

[243] Charles Arthur and Domonic Rushe, *NSA Scandal: Microsoft and Twitter Join Calls to Disclose Data Requests*, THE GUARDIAN (12 June 2013), http://www.theguardian.com/world/2013/jun/12/microsoft-twitter-rivals-nsa-requests; *see also* Ryan Gallagher, *NSA Leaks Suggest Microsoft May Have Misled Public Over Skype Eavesdropping*, SLATE (13 June 2013) http://www.slate.com/blogs/future_tense/2013/06/13/nsa_surveillance_leaks_suggest_microsoft_may_have_misled_public_on_skype.html.

[244] *See* Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN (July 12, 2013), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data; *see also* Jack Clark, *Microsoft: NSA Security Fallout 'Getting Worse' ... 'Not Blowing Over,'* THE REGISTER (June 19, 2014, 6:30 PM), http://www.theregister.co.uk/2014/06/19/microsoft_nsa_fallout/.

between the interest of free speech and the derivative privacy right to be forgotten, or now, "erased".

When one analyzes the "right to be forgotten" in Europe and the United States, one might be struck by the disconnect in shared foundations. In some ways the two continents are speaking languages without a means to translate. In Europe, emerging from a century of intermittent war, the Council of Europe and later the European Union developed protections for the most basic primary concern: the right to family and private life. This protection has grown, despite American influences since the end of World War II, rather than as a result of it. Privacy is explicitly protected in the ECHR, the Charter and national constitutions. The jurisprudence of the Strasbourg Court, and more recently in the Luxembourg Court has developed to raise the interest of data subjects over the interests of those who might process and exploit private information. This right has slowly expanded not only to the collection and use of information, but also the availability of this information to the public as a whole. Other rights, most notably the right to impart and receive information, included in the freedom of expression have been balanced against this right to privacy, often times with a negative result for the freedom of expression.

In the United States, to the contrary, the right to privacy has developed on a different path. In a land where the freedom of expression has become increasingly protected, privacy has developed in its shade. American privacy is protected under two theories, one being based on unenumerated constitutional protections which seek to guard against state intrusions on autonomy rights, while the other seeks to guard against intrusion of privacy rights based upon property rights. This process in many ways is still developing and the struggle remains in determining which information is worth protecting under which theory.

What is needed is a Rosetta Stone of understanding. The days of isolated legal systems that do not take into account alternative systems with disparate concepts of human rights protections are over. The efficiency of communications systems, and to some extent, international trade, require access to the whole story. Yet when one speaks of user posted selfies, ancient misdeeds or malicious ex-lover posts, the information loses some of its importance in a democratic society.

The next question that remains is just how the European Union will proceed on the new regulation. The *Google Spain* case clarified the Court's position, that there is a European "right to be forgotten." Will an emboldened European Union take the Court's message and further expand the right, or will there be a move to limit the potential scope of the right as the Regulation is finalized? Also, going forward, how will search engines such as Google implement the decision? Will they stand as a guardian of information that *ought* to be in the public sphere – that truly informs debate, or will they seek the more cost effective, easier "delete before litigation" path? Let's hope we do not forget what is important.