Kentucky Law Journal

Volume 103 | Issue 3 Article 4

2014

The Right to be Forgotten: Who Decides What the World Forgets?

Patricia Sánchez Abril
University of Miami School of Business Administration

Jacqueline D. Lipton
University of Akron School of Law

The Right to be Forgotten: Who Decides What the World Forgets?

Patricia Sánchez Abril[1]
Jacqueline D. Lipton[2]

ABSTRACT[3]

In May 2014, the Court of Justice for the European Union ("CJEU") surprised the global cyberlaw community by holding that search engines like Google are "controllers" of the processing of personal data under the European Union Data Protection Directive. This means that they are obliged in some circumstances to remove links from search results that pertain to information that infringes on an individual's rights under the Directive. This obligation has come to be referred to as an aspect of a digital "right to be forgotten." The search results in question related to a mortgage sale of property in a bankruptcy that had taken place in 1998. In 2010, links to a Spanish newspaper's advertisement of the sale showed up prominently in Google search results and were no longer relevant and arguably damaging to the data subject.

The case sparked global debate about who should ultimately be responsible for the protection and erasure of private information online. The practical result of the decision leaves much discretion in the hands of online entities, such as Google, Bing, and Yahoo!, to implement their own internal procedures for protecting personal data on the basis of individual complaints made to them. There is little to no governmental or judicial oversight of these procedures.

This Article examines the impact of the recent CJEU decision on global privacy protection. In particular, it canvasses questions about who should bear responsibility for the protection of privacy, ultimately arguing that it is unbefitting and socially undesirable for unchecked businesses to act as the

[1] Associate Professor of Business Law, University of Miami School of Business Administration.

[2] David L. Brennan Professor of Law; Director, Center for Intellectual Property Law and Technology, University of Akron School of Law. The authors would like to thank Professors Eugenio Pizarro Moreno, Lawrence Siry, David Thaw, Dennis Hirsch, Raymond Ku, and all of the editors of the Kentucky Law Journal for their comments and support.

[3] At the time of this writing, the right to be forgotten is a contentious and rapidly-evolving issue in Europe. As such, the authors note that the law described herein is current as of January 2015. At this date, both private and governmental working groups have been assembled to work on a coordinated approach and policies for handling takedown requests.

ultimate arbiters of privacy. However, the pendulum may now have swung so far in this direction that the only meaningful approach to protecting online privacy going forward is for governments and interest groups to assist such businesses in making appropriate privacy-protective decisions.

INTRODUCTION

Since the dawn of the Internet age, possibly even before, legal scholars, philosophers, and others have raised concern about the impact on society of technology that allows details of an individual's life, including successes and missteps, to be generally available to others.[4] As sophisticated search engines like Netscape, and more recently Google, Bing, and Yahoo!, developed, these concerns took on a new level of reality. Any youthful mistakes suddenly became infinitely available and easily searchable online. Even innocent activities that may be embarrassing or humiliating took on a much more ominous significance.

There have also been many stories, some true and some likely urban myths, about people who have been adversely impacted in terms of employment searches, insurance benefits, education, and the like, as a result of information found online that may be inaccurate or out-of-date. One of the worst risks with such information is that a data subject may not ever become aware of what caused the problem if a prospective employer or insurer, for example, does not disclose the contribution of online information in a decision adverse to a data subject's application.[5]

Truthful information, untruthful information, out-of-date information, or information taken out-of-context may harm an individual in a variety of ways, including general reputational harm, bullying, harassment, lack of employment prospects, etc. The scope of the potential damage from the widespread availability of such information is hard to quantify or qualify. Additionally, the information itself as the source of the harm can, in some cases, be hard to pinpoint or prove in litigation. Even where the harm can be quantified and traced to specific online information, many jurisdictions, notably the United States, do not have powerful privacy laws under which an individual may seek redress for the damage.

The advent of the Internet prompted many to take the view that this new technology spelled the death of privacy.[6] A number of commentators said that

[4] *See, e.g.*, DAVID BRIN, THE TRANSPARENT SOCIETY 5–8 (1998) (summarizing ways in which digital technology enables widespread access to an individual's personal data); SHERRY TURKLE, ALONE TOGETHER 252–56 (2011) (describing ways in which teenagers share personal information widely with modern online social media services).

[5] *See* Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First -Century Employee*, 49 AM. BUS. L.J. 63, 87–88 (2012).

[6] *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1465 (2000) (discussing the "rapid growth of privacy-destroying technologies," including databases relying on information collected via the Internet, and the effects on informational privacy); Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538 (quoting Scott McNealy, the CEO of Sun Microsystems saying "You have zero privacy anyway. . . . Get over it.").

society would have to adjust to the lack of privacy on the Internet rather than expect laws to develop to protect a right to privacy.[7]

Nevertheless, many European jurisdictions did not accede to this view. The European Convention on Human Rights protects privacy as a basic human right.[8] The European Union Data Protection Directive ("EU Privacy Directive"),[9] adopted in 1995, requires "controllers"[10] of personal data processing activities[11] to adhere to certain standards with respect to the processing, dissemination, and accuracy of the information,[12] as well as consent by the data subject to processing of certain classes of information.[13] In 2012, the European Union Commission ("EU Commission") went even further in presenting a proposal for a new General Data Protection Regulation ("GDPR") that, amongst other things, specifically includes a right to be forgotten.[14]

This provision requires a controller to erase certain personal data, to preclude further dissemination of the data, and to oblige third parties (such as search engines) to delete links to such data.[15] While the GDPR will not be implemented until 2015, some have argued that the right to be forgotten already appears in a different guise in the current EU Privacy Directive.

This view was borne out by the Court of Justice of the European Union ("CJEU") in May of 2014 in the case of *Google Spain v. Agencia Española de Protección de Datos.*[16] In this case, the CJEU held that a search engine like Google could be classified as a controller of personal data processing and may be obliged to delete certain search results that were out-of-date or irrelevant to the purposes for

---

[7] *See* Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1675–76 (2008).

[8] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR], *available at* http://www.echr.coe.int/Documents/Collection_Convention_1950_ENG.pdf.

[9] 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, 1995 O.J. (L 281) 31, *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=313007.

[10] *Id.* art. 2(d), at 38 ("'[C]ontroller' shall mean 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 . . . .").

[11] *Id.* art. 2(b) ("'[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.").

[12] *Id.* arts. 6–8, at 40–41.

[13] *Id.* arts. 7(a), 8(2)(a), at 40.

[14] *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, art. 17, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *GDPR*], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[15] *Id.*

[16] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=66245.

which they were originally processed.[17] The practical result of the decision has been to place a burden on many global, information-processing businesses to implement procedures to protect individual personal data. The question has arisen as to whether such procedures, with little to no governmental or judicial oversight, are the most appropriate and socially-desirable method for protecting privacy.

This Article considers the impact of the CJEU decision on digital privacy. It recounts the right to be forgotten's controversial and unusual, but successful, legal trajectory in both the national and European legislatures and courts. Against this backdrop, this Article argues that while businesses are socially and practically unfit to become the ultimate arbiters of privacy, they may now have been effectively thrust into that unenviable position. If courts themselves struggle in setting the boundaries between freedom of expression and dignity, between what the public should know and its prurient curiosity, imagine the difficulties faced by businesses in shifting that qualitative—and socially vital—determination to them.

Part I memorializes the history of the right to be forgotten from academic, legislative, and judicial angles. This section culminates at a distinct moment, when, under a crescendo of complaints to the Spanish Data Protection Authority, a Spanish court refers a central question to the CJEU: Do the data processing activities of a search engine like Google make it responsible for the on-demand erasure of people's personal data? Part II examines the ensuing CJEU decision, which answered that question in the affirmative, thereby unleashing waves of surprise, celebration, concern, and confusion. Part III considers the impacts of the decision on digital, information-based business practices and whether placing the burden to protect an individual's right to be forgotten on such businesses is appropriate or even effective in practice, and whether there are currently any meaningful alternatives. Part IV concludes.

The authors note that we have premised the discussion on the idea that a right to be forgotten is an important social value in a digital world. Even if we are wrong on this point, the European Union will continue promoting and protecting the right and its action will force governments and businesses globally to reconsider their role in the protection of individuals from harm relating to outdated, irrelevant, or inaccurate information.

I. HISTORY OF THE RIGHT TO BE FORGOTTEN

The right to be forgotten had a bold and unusual evolution. It was borne of the European notion that privacy is fundamentally a personality right predicated on dignity, attached to a person rather than to his or her property.[18] We see this concept reflected in multiple areas of European law, from Europe's general understanding of intellectual property from a Hegelian personality perspective, to

[17] *Id.*

[18] *See* Karen Eltis, *Breaking Through the "Tower of Babel": A "Right to Be Forgotten" and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 92–93 (2011).

Europe's criminal law.[19] From this conceptual point of departure, Spain—ground zero for the right to be forgotten—jurisprudentially wove what is today known as a new right.

According to Spanish legal scholars, the right to be forgotten is an "atypical assumption in the sense that, as of today, it lacks legal formulation and is of limited dogmatic heft."[20] The right has been described as developing through the Spanish courts and legislature in a "slow and, clumsy, yet daring fashion."[21] In fact, it does not appear to be specifically provided or granted by any article of Spanish or international law.[22] Instead, legal scholars and judges have read it as implicit in various sections of the EU Privacy Directive and Spain's 1999 domestic data protection law.[23] And legislators have followed suit. The following paragraphs describe the right's intrepid evolution.

Legal Scholarship

As is the tradition in civil law, the writings of legal scholars provided early impetus for the eventual formation of the right. In 1991, a Spanish scholar first alluded to what he called a modern right to be forgotten.[24] Professor O'Callaghan foresaw that certain information flow—and its logical inferences—could harm an individual's right to privacy if unchecked. He spoke in particular of the case in which information from a distant time or place is unearthed in the present day to sully its subject's character.[25]

Ironically, Professor O'Callaghan and others attribute the birth of the distinctly European right to a well-known American privacy case,[26] *Melvin v. Reid*.[27] In this often-cited 1931 California case, a woman named Gabrielle Darley sued a film company that made a motion picture about her previous salacious affairs.[28] Darley

---

[19] Ashley Messenger, *What Would a "Right to Be Forgotten" Mean for Media in the United States?*, COMM. LAW., June 2012, at 29, 29–30, 35. France, Germany, Switzerland, Spain, and the United Kingdom all recognize a right to remove data about convicted criminals. *Id.* at 29–30. In France this was known as *le droit à l'oubli*, a predecessor in both name and form to the modern digital counterpart. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf.

[20] Patricia S. Abril & Eugenio Pizarro Moreno, *La Intimidad Europea Frente a la Privacidad Americana: Una Visión Comparativa del Derecho al Olvido*, INDRET: REVISTA PARA EL ANÁLISIS DEL DERECHO, Jan. 2014, at 1, 25 (translated by author), *available at* http://www.indret.com/pdf/1031.pdf.

[21] *Id.* at 28 (translated by author).

[22] *Id.*

[23] *See* Protection of Personal Data art. 7 (B.O.E. 1999, 298) (Spain); *GDPR*, *supra* note 14, art. 17.

[24] XAVIER O'CALLAGHAN MUÑOZ, LIBERTAD DE EXPRESIÓN Y SUS LÍMITES: HONOR, INTIMIDAD E IMAGEN 54 (1991).

[25] *Id.* at 55.

[26] *Id.* at 54–55 (citing PABLO SALVADOR CODERCH ET AL., ¿QUÉ ES DIFAMAR? LIBELO CONTRA LA LEY DEL LIBELO 97 (1987)).

[27] 297 P. 91 (Cal. Dist. Ct. App. 1931).

[28] *Id.* at 91.

had once been a prostitute accused—but later acquitted—of murder.[29] According to the case, in 1918, she "abandoned her life of shame and became entirely rehabilitated," marrying and "assum[ing] a place in respectable society."[30] Seven years later, a film named "The Red Kimono" about Darley's previous life was released and advertised using Darley's full, real name.[31] Stretching for a legal ground to protect this now-virtuous woman, the pitying California court held that even though some of her past was contained in the public record (and thus could not deemed private), the use of Darley's true maiden name in conjunction with the film and its advertisement constituted a "direct invasion of her inalienable right . . . to pursue and obtain happiness."[32]

The decision stands on firmer moral and policy grounds than it does on legal footing. In fact, the court repeatedly defended its holding by citing the need to incentivize rehabilitation and reward social reformation.[33] Today, any shred of this case remaining in U.S. privacy law can be found in the public disclosure tort, which prohibits the unauthorized disclosure of truthful, offensive, private facts that are not of public concern.[34] This California case evidently had a more meaningful legal impact abroad in the formation of the right to be forgotten, almost a century later.

Governing Legislation

Any student of the right to be forgotten must have at least a cursory understanding of the thicket of treaties and supranational and national laws that undergird the incipient right:

Article 16 of the Consolidated Treaty on the Functioning of the European Union (TFEU).[35] As introduced by the Lisbon Treaty, Article 16(1) establishes the principle that "everyone has the right to the protection of personal data concerning [him or her]."[36] Article 16(2) in the Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data.[37]

Articles 1, 7, and 8 of the European Union's Charter of Fundamental Rights.[38] Title 1, Article 1 of this supreme charter simply states that "[h]uman dignity is

---

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.* at 93.

[33] *See id.*

[34] *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[35] Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2012:326:FULL&from=EN.

[36] *Id.* art. 16(1).

[37] *Id.* art. 16(2).

[38] Charter of Fundamental Rights of the European Union arts. 1, 7–8, Dec. 7, 2000, 2007 O.J. (C 303) 1 [hereinafter Charter of Rights], *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2007:303:FULL&from=EN.

inviolable. It must be respected and protected."[39] Article 7 secures respect for "private and family life, home and communications."[40] Article 8 governs personal data, granting a data subject protection, and the right to consent, access, and rectify personal information.[41]

Article 8 of the European Convention for Human Rights ("ECHR").[42] Under its Article 8, the ECHR states that "[t]here shall be no interference by a public authority with the exercise of this right [to private life] except such as is in accordance with the law."[43] The Convention ensures a European citizen "the right to respect for his private and family life, his home and his correspondence."[44] The fundamental right to privacy has been incorporated into the laws of EU member states.[45] The European Court of Human Rights interprets the Convention, tending toward a privacy-protective stance.

Articles 5, 6, 8, and 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[46] When it became apparent that the protection of the ideals of Article 8 of the ECHR required specific and systematic development, the Council of Europe prepared what is known as Convention 108 to safeguard principles of data quality and privacy, and to require member nations to adopt mirroring national measures.[47] Article 5 governs data quality, lawful collection, and storage.[48] Article 6 provides that "[p]ersonal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life may not be processed automatically unless domestic law provides appropriate safeguards."[49] Article 8 provides the data subject with avenues for information collection and redress regarding the maintenance of personal data.[50] Article 9 enumerates exceptions, including "state security," protection of "the data subject," and protection of "the rights and freedoms of others."[51]

1995 European Union Data Protection Directive (Privacy Directive).[52] The

[39] *Id.* art. 1.

[40] *Id.* art. 7.

[41] *Id.* art. 8.

[42] ECHR, *supra* note 8, art. 8. The ECHR was formerly the Convention for the Protection of Human Rights and Fundamental Freedoms.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data arts. 5–6, 8–9, Jan. 28, 1981, 1496 U.N.T.S. 65, *available at* https://treaties.un.org/doc/Publication/UNTS/Volume%201496/volume-1496-I-25702-English.pdf.

[47] *See id.* pmbl.

[48] *Id.* art. 5.

[49] *Id.* art. 6.

[50] *Id.* art. 8.

[51] *Id.* art. 9.

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

Directive provides the foundation for the European Union's well-developed privacy law. The Directive introduced into law the principle that personal data can only be processed when it meets certain conditions relating to transparency, legitimate purpose, and proportionality, and requires each member state to set up a supervisory authority.[53] Of particular interest to the study of the right to be forgotten, the Privacy Directive's Article 12(b) provides that "Member States shall guarantee every data subject the right to obtain from the controller: as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data."[54]

> This right is subject to each member state's exemptions "for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[55]
>
> The Directive has undergone a series of updates. Most notably, in 2002, the Directive on Privacy and Electronic Communications, also known as the E-Privacy Directive, continued to update earlier efforts, covering the confidentiality of information, traffic data, spam, and cookies.[56] The Privacy Directive reacted to "[p]ublicly available electronic communications services over the Internet," which "open new possibilities for users but also new risks for their personal data and privacy."[57] The specific portions of the Directive implicating the right to be forgotten are discussed in the following section.
>
> The Directive continued to react to evolving technologies, continually seeking to implement and improve on its regulatory frameworks. In 2011, the European Data Protection Supervisor issued an opinion giving the national data protection agencies the authority to regulate and sanction data protection violations on a national level.[58]

Soon enough, as European citizens issued complaints to their national authorities, it became clear that there was a clamoring for the ability to delete personal digital information. In early 2012, Viviane Reding, European Commissioner for Justice, Fundamental Rights, and Citizenship, introduced the right to be forgotten.[59] She explained that the novel privilege would give Europeans

---

[53] *See id.* arts. 7, 28.

[54] *Id.* art. 12(b).

[55] *Id.* art. 9; *cf.* Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, 2008 E.C.R. I-09831 (interpreting Council Directive 95/46, 1995 O.J. (L 281) 31 (EC)).

[56] Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), arts. 5–6, 13–14, 2002 O.J. (L 201) 37, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.

[57] *Id.* at 37.

[58] *Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council Establishing Technical Requirements for Credit Transfers and Direct Debits in Euros and Amending Regulation* (EC) No 924/2009, 2011 O.J. (C 284) 1, 2–3, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:284:0001:0004:En:PDF.

[59] Viviane Reding, Vice President, European Comm'n, EU Justice Comm'r, The EU Data

"the right—and not only the 'possibility'—to withdraw their consent to the processing of the personal data they have given out themselves."[60] Essentially, "[i]f an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system."[61] Commissioner Reding made clear that the right to be forgotten is not an absolute right that can "amount to a right of the total erasure of history" or should "take precedence over freedom of expression or freedom of the media."[62]

Days after Reding's speech, the right to be forgotten was outlined in Article 17 of the proposed GDPR.[63] As drafted, the GDPR gives data subjects:

> [T]he right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
>
> (a) [T]he data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) [T]he data subject withdraws consent on which the processing is based . . . or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
>
> (c) [T]he data subject objects to the processing of personal data . . . ;
>
> (d) [T]he processing of the data does not comply with this Regulation for other reasons.[64]

The GDPR emphasizes that the right to be forgotten is particularly relevant in cases "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."[65]

The GDPR sketches only faint boundaries for the right to be forgotten: it may not apply where data retention "is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them."[66] Article 80 creates an exemption for "journalistic purposes . . . in order to reconcile the right

---

Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5 (Jan. 22, 2012), *available at* http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *GDPR*, *supra* note 14, art. 17.

[64] *Id.* art. 17(1); *see also infra* Appendix A for full text of art. 17.

[65] *GDPR*, *supra* note 14, at 25, ¶ 53.

[66] *Id.*

to the protection of personal data with the rules governing freedom of expression" in accordance with Article 9 of the Privacy Directive.[67]

The GDPR is the first legislative expression of the right to be forgotten.[68] Through it, individuals can request the erasure of their digital data, including photographs. The GDPR establishes obligations according the subjects' roles in the information flow process. Of critical importance is the designation of controller. For example, the person (or entity) responsible for the original publication must suppress the data and refrain from further diffusion.[69] The party responsible for publishing the data must erase it and inform any third party that touches the data to follow suit.[70] At this writing, it is expected that the GDPR's legislative process will conclude in 2015, and EU Member States will then have an additional two years of transition to the new rules. Although the GDPR will not go into full effect until 2017 (at the earliest), the right to be forgotten has already established a footing in European case law, as we examine in the next section.

Spanish and European Case Law

Against this academic and legislative backdrop, the Spanish judiciary slowly began accepting the right to be forgotten, as it began bubbling up in the lower courts at the end of the 2000s. Unlike the United States, where First Amendment concerns could have trumped any case in which an individual sought to silence his past,[71] Spanish courts, like those of other European Union countries, engage in a proportional balancing of equal constitutional rights—say, between the right to freedom of expression and the fundamental right to privacy—in deciding cases.[72] That is, when two constitutional rights collide, no clear interpretive guidance exists on the hierarchy of rights: courts must balance the right to privacy against the right to freedom of expression on a case-by-case basis. However, Spanish courts have often capitulated to privacy interests where they determine that time has made the noxious information irrelevant (or, in American legal terminology, not of legitimate public concern) or outdated.

In practically forming the right, Spanish courts have also taken direction from European courts ruling on digital information disclosure. In particular, in 2010, the European Court of Justice (ECJ, the precursor to the CJEU) examined whether

---

[67] *Id.* art. 80.

[68] *See* FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12), EUROPEAN COMM'N (2014), *available at* http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data factsheet_data_protection_en.pdf.

[69] *See GDPR*, *supra* note 14, art. 17; *see also infra* Appendix A for full text of art. 17.

[70] *See GDPR*, *supra* note 14, art. 17.

[71] *See, e.g.*, Daniel Fisher, *Europe's "Right to Be Forgotten" Clashes with U.S. Right to Know*, FORBES (May 16, 2014, 8:45 AM), http://www.forbes.com/sites/danielfisher/2014/05/16/europes-right-to-be-forgotten-clashes-with-u-s-right-to-know; Craig Timberg & Sarah Halzack, *Right to Be Forgotten vs. Free Speech*, WASH. POST (May 14, 2014), http://www.washingtonpost.com/business/technology/right-to-be-forgotten-vs-free-speech/2014/05/14/53c9154c-db9d-11e3-bda1-9b46b2066796_story.html.

[72] *See* Charter of Rights, *supra* note 38, art. 52.

European Union legislation requiring the publication of personal data (for administrative purposes) contravened European Union privacy dictates.[73] Plaintiffs complained that they suffered privacy harm when the Internet site of the German Federal Office for Agriculture and Food identified them by name as beneficiaries of agricultural aid without their consent.[74] The site also disclosed their addresses, the annual amounts they received, and contained a search tool.[75] Although the noble aim of the legislation was to increase transparency regarding the use of public funds, the ECJ chastised the implementing institutions, accusing them of a failure in balancing the objectives of the law with the protection of personal data embodied in Articles 7 and 8 of the Charter.[76] According to the ECJ, similar goals may have been attained with alternative publication methods, such as anonymized information.[77] The court invalidated the regulation as overbroad and violative of fundamental privacy rights.[78] This case provides an important example of the balancing that European national and supranational courts require when determining privacy interests, as well as their penchant for privacy.

But privacy interests do not always win the day against freedom of expression. In 2011, the first right to be forgotten case in Spain was brought forth in the national tribunal by an attorney and former judge who brought suit against both Spain's Constitutional Court[79] and the newspaper *Diario El Pais* for removal of all reference to his name on their respective websites.[80] The Spanish Data Protection Agency had denied bringing a case on the plaintiff's behalf.[81] The two websites contained references to the attorney's 1979 conviction for forgery, which he claimed were causing continuing harm to his professional reputation.[82] The plaintiff's arguments failed on both counts. The court held that freedom of expression trumped privacy in this case, where truthful information of public concern was legally published and captured online.[83] Moreover, the Spanish Constitutional Court was under a legal obligation to report its cases. After failing, the plaintiff went on to sue Google. Other similar cases followed with varying

---

[73] Joined Cases C-92/09 & C-93/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] The Constitutional Court of Spain is a tribunal that serves as "the supreme interpreter of the Spanish Constitution." *Competences*, TRIBUNAL CONSTITUCIONAL DE ESPAÑA, http://www.tribunalconstitucional.es/en/tribunal/competencias/Pages/Competencias.aspx (last visited Feb. 5, 2015). It is independent of the Spanish judiciary system and is distinct from the Spanish Supreme Court. *Id.*

[80] S.A.N., May 12, 2011 (A.N., No. 2370) (Spain), *available at* http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=5987513&links=&optimize=20110602&publicinterface=true.

[81] *Id.*

[82] *Id.*

[83] *Id.*

degrees of success in the Spanish courts.[84]

From 2011 to 2013, complaints to the Spanish Data Protection Agency proliferated. A campground named Alfaques, where a deadly tanker explosion had occurred in 1978, sued to remove prominent links to news stories of the disaster, reasoning that this history was bad for business.[85] A plastic surgeon named Hugo Guidotti sought the removal of a link to a 1991 newspaper story entitled "The Risk of Wanting to be Slim," which chronicled a five million Euro malpractice lawsuit against him.[86] (Because he won the suit, he objected to the dated article's characterization of him.)[87] Ultimately, the Spanish Data Protection Agency ordered Google to remove links to online news articles in over ninety cases.[88] In its defense, Google rebutted that Spain was the only country requiring it to remove links that were not per se illegal.[89]

Without a direct governing law on the right to be forgotten, Spanish courts were left to piece together the extant Privacy Directive for guidance. The definitive case became *Google Spain SL v. Agencia Española de Protección de Datos.*[90] When an Internet user entered plaintiff Mario Costeja Gonzalez's name in a Google search engine, the searcher was presented with links to pages of the *La Vanguardia* newspaper from 1998 that contained an announcement listing Costeja's name in connection with a real-estate auction in a bankruptcy proceeding.[91] The newspaper was also a defendant in the action, but was ultimately held not to be liable with respect to the right to be forgotten because it legally published the advertisement.[92] In 2010, the Spanish Data Protection Director, in an administrative proceeding, ordered Google Spain and Google, Inc. to adopt the necessary measures to erase the data from its index and to render their future access impossible.[93] Google Spain and Google, Inc. appealed.

Struggling with these issues on appeal, the *Audiencia Nacional* (Spanish

[84] *See, e.g.*, S.A.N., Apr. 29, 2011 (A.N., No. 2140) (Spain), *available at* http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=5966837&links=&optimize=20110519&publicinterface=true.

[85] S.A.P., Oct. 2, 2012 (A.P., No. 1671) (Spain), *available at* http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6600300&links=alfaques&optimize=20130112&publicinterface=true.

[86] Paul Sonne et al., *Plastic Surgeon and Net's Memory Figure in Google Face-Off in Spain*, WALL ST. J. (Mar. 7, 2011, 12:01 AM), http://online.wsj.com/article/SB10001424052748703921504576094130793996412.html.

[87] *Id.*

[88] Ciaran Giles, *Spain Launches First 'Right to Be Forgotten' Case Against Google*, HUFFINGTON POST (June 21, 2011, 5:12 AM), http://www.huffingtonpost.com/2011/04/21/right-to-be-forgotten-google-spain_n_851891.html.

[89] Ciaran Giles, *Google appeals Spanish demand to take down links*, Associated Press (January 19, 2011, 11:17 AM), http://news.yahoo.com/google-appeals-spain-mandate-down-links-20110119-065054-473.html.

[90] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=66245.

[91] *Id.* ¶ 14.

[92] *Id.* ¶ 16.

[93] *Id.* ¶ 2.

National High Court) referred to the CJEU some perplexing legal questions regarding the proper interpretation of Google's obligations to the public under the Privacy Directive. Since the Directive was written before the days of search engines, the court reasoned, more guidance was necessary regarding their role vis-a-vis the mandatory suppression of certain digital information by its controllers.[94] The Spanish court referred three main questions to the CJEU:

> 1. Whether the activities of Google Inc. and the Spanish subsidiary brought the search engine within the territorial scope of the Directive;
>
> 2. If so, whether the activity of the search engine in collecting, caching, indexing and retrieving data constituted "processing" under the Directive, for which the search engine would be the data controller; and,
>
> 3. If so, whether the individual could invoke rights under the Directive to seek erasure or object to processing to have the data removed. Could individuals ask search engines to suppress information that was legally published on the basis of their subjective belief that such information "could harm them" and/or their "desire that such information be forgotten"?[95]

The pending questions for the CJEU understandably caused much chatter and consternation between both European Union and global watchers. The final CJEU decision would be eagerly awaited.

In the interim, the Advocate-General Nillo Jääskinen of the CJEU, delivered an influential, but not binding, opinion on the three central questions of the case.[96] On the first question, the Advocate-General opined that Google, Inc. fell within the territorial scope of the Privacy Directive regardless of whether it processed personal data within Spanish territory.[97] On the second question, he opined that search engines were not controllers of personal data from websites and thus national data protection authorities did not have the power to require an Internet search engine service provider to withdraw indexed information.[98] Finally, on the third burning question, Advocate-General Jääskinen argued that the Directive does not establish a right to be forgotten; the Directive's rights to data rectification, erasure, and blocking, according the Advocate-General, only concerned data whose processing does not comply with the Directive.[99] In sum, the opinion stated,

---

[94] *Id.* ¶¶ 20–21.

[95] *See id.* ¶ 20.

[96] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (June 25, 2013) (Advisory Opinion of Advocate-General Nillo Jääskinen) [hereinafter Jääskinen Advisory Opinion], http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=758120; Press Release No. 77/13, Court of Justice of the European Union, Advocate General Jääskinen Considers That Search Engine Service Providers Are Not Responsible, on the Basis of the Data Protection Directive, for Personal Data Appearing on Web Pages They Process (June 25, 2013) [hereinafter Press Release No. 77/13], *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf.

[97] Jääskinen Advisory Opinion, *supra* note 96, ¶ 64.

[98] *Id.* ¶ 89.

[99] *Id.* ¶¶ 136–137.

"subjective preference alone does not amount to a compelling legitimate ground and thus the Directive does not entitle a person to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests."[100] Many considered this interim opinion indicative of the CJEU opinion to come, but that was not to be the case.

II. *GOOGLE SPAIN V. COSTEJA GONZÁLEZ*: THE CJEU HOLDING

In *Google Spain SL v. Agencia Española de Protección de Datos*, Google Inc., headquartered in the United States, was a party to the action and Google's American operations were affected by the court's decision.[101] As noted in the Introduction, the proposed GDPR will implement an express right to be forgotten into European Union law. In the meantime, the CJEU has created virtually the same right in its recent interpretation of rights already existing under the 1995 law: the laws enacted throughout European Union member states under the EU Privacy Directive.[102]

1. Is Google a controller of personal data processing activities?—The CJEU was asked to consider whether Google could be regarded as a controller of personal data processing activities under the Privacy Directive in circumstances where a Spanish national (Costeja González) complained about specific Google search results.[103] For the purposes of the Directive, "processing of personal data" or "processing" is defined 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 . . . ."[104] Under the Directive, controller is defined 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 . . . ."[105] The definition of personal data[106] was not particularly problematic in its application to this case because it broadly relates to large classes of information pertaining to an individual data subject, and

[100] Press Release No. 77/13, *supra* note 96.

[101] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos ¶¶ 43–60 (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=66245.

[102] *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) (discussing recent CJEU interpretation of the Directive in the following sections).

[103] *Google Spain*, Case C-131/12, ¶ 20.

[104] Council Directive 95/46, art. 2(b), 1995 O.J. (L 281) 31 (EC).

[105] *Id.* art. 2(d).

[106] The Privacy Directive defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.* art. 2(a).

information specifically naming the complainant in the context of a bankruptcy sale undeniably met the requirements of the definition.[107]

With respect to the question of whether Google was involved in data processing activities within the meaning of the Directive, the CJEU followed previous precedent in holding that the operation of loading personal data onto an Internet page is a processing of data within the meaning of the Directive.[108] The CJEU further noted that Google's activities also involved collecting, retrieving, recording, organizing, storing, disclosing, and making available to its users (in the form of search results) personal information about data subjects.[109]

These are precisely the activities regulated by Article 2(b) of the Directive and thus Google was unquestionably engaged in the processing of personal data under the Directive. It was irrelevant that Google also carried out the same operations with respect to other types of information and did not treat personal data any differently from other information indexed by its search engine functions.[110] Further, the CJEU held that it was irrelevant that the information in question had already been published online by *La Vanguardia* and was not altered by Google.[111]

With respect to whether Google should be classified as a controller of the data processing activities under the Directive, the CJEU noted that Google is a body that "determines the purposes and means of the processing of personal data" for the purposes of Article 2(d) of the Privacy Directive.[112] These purposes and means may well differ from those of the website on which the information was originally posted and still satisfy the provisions of Article 2(d).[113] In this case, the purposes and means of processing in a search engine are different from *La Vanguardia*'s processing and means to advertise the bankruptcy auction.[114]

2. Legal Obligations of a controller of personal data processing activities.— Holding that Google was a controller of data processing activities under the Privacy Directive was, of course, not the end of the story. The CJEU was then required to examine the obligations imposed on controllers under the Directive.[115] The Court specifically considered the obligations set out in Articles 6 and 12 of the Directive.[116] Article 6(1) provides that:

> Member States shall provide that personal data must be:

[107] *Google Spain*, Case C-131/12, ¶ 27 ("[I]t is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of [the Privacy Directive].").

[108] *Id.* ¶ 26.

[109] *Id.* ¶ 28.

[110] *See id.*

[111] *Id.* ¶¶ 29, 31.

[112] *Id.* ¶¶ 32–33.

[113] *Id.* ¶ 35.

[114] *Id.* ¶¶ 14, 16, 35.

[115] *Id.* ¶ 19.

[116] *Id.* ¶¶ 7, 10.

> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[117]

Article 6(2) provides that it is the responsibility of the controller to ensure compliance with the requirements set out in Article 6(1).[118] Article 12(b) of the Directive further provides a right for a data subject to obtain from a controller: "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[119]

In order to achieve a balance between the rights of those involved in data processing and the privacy rights of data subjects, the Directive also includes a provision that allows for processing of personal data under certain circumstances. Article 7 provides that:

> Member States shall provide that personal data may be processed only if:
>
> (a) the data subject has unambiguously given his consent; or . . .
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or . . .
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject . . . .[120]

In *Google Spain*, the CJEU addressed the balance between the search engine's legitimate interests under Article 7(f) and the data subject's right to privacy.[121]

[117] Council Directive 95/46, art. 6(1), 1995 O.J. (L 281) 31 (EC).

[118] *Id.* art. 6(2).

[119] *Id.* art. 12(b).

[120] *Id.* art. 7.

[121] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos ¶ 74 (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclan

Ultimately, it held that the economic interests of a private corporation like Google could not override the data subject's privacy rights.[122] The CJEU also rejected Google's argument that a data subject like Costeja should be required to request removal from the original third party website that published the information (*La Vanguardia*'s website) rather than to seek redress directly from Google at the same time:

> Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.[123]

Thus, it was unnecessary for the injured party (Costeja) to seek removal of the information from *La Vanguardia*'s website prior to seeking action from Google Spain.

The CJEU further noted that an original third party website may have different reasons for processing information than a search engine and may be excused for its processing activities under the Privacy Directive. For example, a newspaper website, such as *La Vanguardia*, may be excused in its processing of personal information if that processing is carried out "solely for journalistic purposes" under Article 9 of the Directive, which expressly balances the right to privacy against other important social values such as freedom of expression.[124] Thus, Google could be required to remove links to information published on third party websites that contain personal information that is inaccurate, irrelevant, or excessive,[125] even where the links are lawful on the third party website. The publication by *La Vanguardia* in 1998 of information about the mortgage sale was accurate and relevant.[126] However, a linking sixteen years later to that information in search results did not meet that standard and was regarded as being published only for Google's own commercial purposes.[127]

In making this determination, the CJEU noted that in some situations, for example where the data subject played a prominent role in public life, interference with his fundamental rights may be justified by the "preponderant interest of the general public in having . . . access to the information in question."[128] However,

---

g=en&mode=lst&dir=&occ=first&part=1&cid=66245.

[122] *Id.* ¶ 81 ("In light of the potential seriousness of [interference with a data subject's privacy rights], it is clear that it cannot be justified by merely the economic interest which the operator of a search engine has in that processing.").

[123] *Id.* ¶ 84.

[124] *Id.* ¶ 85.

[125] *See id.* ¶ 93.

[126] *See id.* ("[E]ven initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.").

[127] *Id.* ¶ 98–99.

[128] *Id.* ¶ 97.

that was not the case on the facts of *Google Spain*. In cases where a private individual's fundamental rights are being infringed, neither the economic interests of a search engine nor the interest of the general public in accessing the information should override the data subject's privacy right.[129]

III. IMPACTS AND IMPLICATIONS OF THE DECISION: WHO DECIDES WHAT THE WORLD WILL FORGET?

The most obvious impact of the CJEU decision in *Google Spain*, which will be reinforced when the GDPR is implemented throughout the European Union, is that a heavy burden will be placed on online intermediaries such as search engines, potentially also social networking services, and other popular Internet services to police the right to be forgotten. Soon after the *Google Spain* decision, Google implemented a webform for processing removals. In the first months, the company reportedly received 135,000 requests for erasure referring to 470,000 links, mostly from Britain, France, and Germany.[130] Throughout the summer and fall of 2014, Google and other search engines worked with the Article 29 Working Party, a European Commission advisory group comprised of representatives of each European Union country's data protection authority, to establish the implementation of the *Google Spain* decision.[131] The logistics for online erasure, as well as the work of the advisory group, are at a critical point in their evolution. Their conclusions and procedures will likely influence privacy practices in Europe, and potentially globally, for years to come. For this reason, we must look closely at the impacts of *Google Spain*.

This section argues that the CJEU decision places an undue burden on online intermediaries, which become the ultimate arbiters of privacy without judicial or governmental assistance or oversight. This role involves an unbefitting qualitative assessment, and carries considerable legal, social, and practical ramifications.

1. The Anatomy of an Erasure: What Online Intermediaries Must Consider in Determining Privacy.—In a recent questionnaire, the Article 29 Working Party asked Google and other search engines what criteria they use to balance their "economic interest and/or the interest of the general public in having access to . . . information versus the right of the data subject to have search results delisted."[132] Google responded as follows, in relevant part:

---

[129] *Id.* ¶ 99.

[130] *The Right to Be Forgotten: Drawing the Line*, ECONOMIST, Oct. 4, 2014, http://www.economist.com/news/international/21621804-google-grapples-consequences-controversial-ruling-boundary-between.

[131] Press Release, Article 29 Data Prot. Working Party, European DPAs Meet with Search Engines on the "Right to Be Forgotten" (July 25, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf.

[132] Letter from Peter Fleischer, Global Privacy Counsel, Google, to Isabelle Falque-Pierrotin, Chair, Article 29 Working Party (July 31, 2014), *available at* http://online.wsj.com/publicresources/documents/google.pdf.

> When evaluating requests, we will look at whether the search results in question include outdated or irrelevant information about the data subject, as well as whether there's a public interest in the information.
>
> In reviewing a particular removal request, we will consider a number of specific criteria. These include the individual (for example, whether an individual is a public figure), the publisher of the information (for example, whether the link requested to be removed points to material published by a reputable news source or government website), and the nature of the information available via the link (for example, if it is political speech, if it was published by the data subject him—or herself, or if the information pertains to the data subject's profession or a criminal conviction).[133]

The final point about criminal convictions was recently considered by a Dutch court when reviewing Google's refusal to remove links pertaining to the owner of an escort agency who was convicted for six years' imprisonment in 2012 with respect to an attempted incitement for a contract killing.[134] The Dutch court, applying the ruling from *Google Spain*, upheld Google's refusal to remove the links on the basis of the nature of the information involved, despite the fact that an appeal was pending and the information could be harmful to the complainant in his personal life in the interim.[135]

In coming to its conclusion, the Dutch court was mindful of the need to balance free speech against privacy rights and pointed out that "[t]he [*Google Spain*] judgment does not intend to protect individuals against all negative communications on the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions."[136] Thus, there will be some situations in which the right to free expression will trump the right to privacy online.

As other commentators have pointed out, the elements of "being pursued for a long time" and "unnecessarily defamatory" expression are both judicial glosses by the Dutch court on the CJEU's *Google Spain* decision.[137] However, they may provide some clarity to businesses applying the decision in practice. The Dutch court went even further with respect to information pertaining to a serious criminal conviction, holding that "[t]he conviction for a serious crime . . . and the negative publicity as a consequence thereof, in general provide information about an individual that will remain relevant."[138] It would therefore seem that, at least in the

---

[133] *Id.*

[134] Rb. Amsterdam 18 september 2014, KG 2014, 960 m.nt. ZA ([Plaintiff]/Google Neth. BV) (Neth.), *available at* http://uitspraken.rechtspraak.nl/inziendocument?id-ECLI:NL:RBAMS:2014:6118.

[135] *Id.*

[136] Joran Spauwen & Jens van den Brink, *Dutch Google Spain Ruling: More Freedom of Speech, Less Right to Be Forgotten for Criminals*, INFORRM'S BLOG (Sept. 27, 2014), http://inforrm.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink.

[137] *Id.*

[138] *Id.*

cases of information about serious criminal activities, the right to privacy may give way to the right to disseminate the information (or link to websites that disseminate the information in question).

The following subsection examines some of the challenges now facing businesses like Google in making determinations such as those arising under the facts recently considered by the Dutch court. These businesses, with scant guidance from courts and the European regulations, will have to make decisions that significantly affect individuals' privacy and may impact many people's daily lives. Hopefully, the Article 29 Working Party will be helpful in considering these issues and providing some guidance to those business entities, like Google, faced with these determinations on a daily basis.

2. Qualitative Decisions Involved in Determining Privacy.—Entities like Google, Bing, Yahoo!, and many others that handle voluminous amounts of personal data, often through largely automated processes, will now be faced with determinations as to when to erase information or links to information that may infringe the right to be forgotten as contemplated by *Google Spain* and its progeny, and ultimately as reconceived in the forthcoming GDPR. These determinations will include qualitative questions such as:

> (a) whether truthful information should be treated differently to false information and, if so, how to determine which information falls into which category;
>
> (b) how to classify information as "old" versus "new" and at what point does the "staleness" of information require its removal on request by a data subject;
>
> (c) the relevance of the original source of the publication to a removal request.

For example, is information published in a formal news media outlet to be treated differently from that published in a personal blog, social media website, or chat group? The current European laws do not particularly differentiate between true or false information, other than the Dutch court's suggestion that "unnecessarily defamatory" information (presumably a form of false information) not be protected to the same extent as truthful information. Thus, businesses making determinations about what kind of information should be removed and what should be preserved are in an extremely invidious position in terms of regulatory guidance. It may be preferable to err on the side of removal to avoid potential legal liability, but this imposes significant cost burdens on such businesses and effectively sanctions censorship at the behest of an individual who may make a vexatious or non-meritorious complaint about the availability of information.

Perhaps a brief thought experiment will serve to outline how thorny these issues may become in practice. Consider, for example, the facts from the Guidotti case in the Spanish court system.[139] In that case, a plastic surgeon sought the removal of a link to a 1991 newspaper story that detailed a five million Euro

[139] *See supra* Part I.

malpractice suit against him. He won the suit and thus objected to the link that would lead Internet searchers to a dated newspaper article's categorization of his surgical practices. If these facts arose today, would Google (or any other search engine) be required to remove links to the newspaper story? While the story was the result of serious journalism, was published in a mainstream media outlet, and it was factually correct at the time it was published, its continued prominence in search engine results could harm the doctor's reputation and practice in a way that mere publication in a newspaper in 1991 would not. Under today's law, is the article sufficiently outdated and irrelevant to support a removal request, at least with respect to Google, if not to the newspaper's website? What about the Dutch court's view of information that is "irrelevant," "unnecessary," or "unnecessarily defamatory"? Could the dated newspaper article now meet those criterions given that the doctor ultimately won the lawsuit? Thus, continued prominent access by Internet searchers to the information provides an unnecessarily misleading portrait of the doctor in the present day?

An associated question for businesses to consider is how to determine today what information may be relevant in the future. Much of the current discourse relates to outdated information that is *less* relevant now than it may have been in the past. What about information that did not appear particularly noteworthy or important in the past but may become relevant in the future? For example, if we accept that the plastic surgeon is entitled to have his reputation cleansed in light of winning the legal suit, what would happen if his techniques irreparably damaged a patient in the future? Would that reanimate the importance or relevance of the information? Would a search engine that had suppressed links on the basis of the present law face liability for not realizing that the information could become relevant in the future? What if the plastic surgeon subsequently ran for political office and was placed in a prominent position in a department overseeing the health of citizens? Would the information be relevant then on the basis identified in *Google Spain*—that is, the data subject is now playing a role in public life and the interference with his privacy rights is justified by the interest of the public in having access to the information? In other words, could relevance ever be resurrected in light of new events?

Assuming that search engines and other online businesses will now err on the side of acceding to removal requests to avoid legal liability, an assumption that we admit may not be borne out in time, what might the general effects of that practice be on society more generally? Removal of more information might lead to a less rich public discourse overall and might privilege the more educated, sophisticated, or wealthy who are more attuned to the laws that allow them to request reputation cleansing services, and can rely on legal threats to back up their requests.

Interactive, widely-used online services, such as the Google search engine, are very different entities from those to whom the 1995 Privacy Directive were targeted. In the 1990s, most online services that processed data were entities that specifically did so in the course of their businesses, such as educational institutions, health insurance companies, market research companies and the like. Those entities

could be expected to take precautions to protect individual privacy because their activities were specifically targeted at collecting and processing personal data. Many of today's online service providers are a different story, only incidentally processing personal data as part of a much larger operation. Indeed, as noted in Part II, Google argued in *Google Spain* that its processes did not distinguish between personal data and other kinds of data. The search engine was not established specifically to process personal information, although it incidentally does so as part of its larger operations.

Asking entities whose focus is not the processing of personal data to invest in implementing a right to be forgotten is, in some ways, asking for the right to fail in practical terms or to overtake other rights, like freedom of expression, by encouraging entities like Google to err on the side of acceding to removal requests. These entities have also shown that it is unwieldy for them to engage in practices to protect an individual's right to be forgotten and, with little government oversight, they may do a poor job in implementing the right, which may lead to increasing litigation to determine in what circumstances the right to privacy should trump the right to free speech. Hopefully the Article 29 Working Party can provide some guidance and prevent excessive litigation in the future.

At the present time, Google is utilizing a process under which an individual can complain about specific search result links containing irrelevant or outdated information. Google then uses its own internal procedures, which it does not necessarily disclose to the public, in order to make its own determination as to whether the link(s) in question should be removed. Of course, individuals who are not satisfied with Google's actions in a particular case can bring an action, and are in practice bringing actions, under European Union laws. However, this process is expensive, unwieldy, and obviously not globally harmonized. An American citizen, for example, has little legal recourse against a company like Google with respect to the removal of links to damaging, but truthful, information. The disharmonization of privacy law between the United States and the European Union, for example, is more than just a difference in legislation. The laws in question reflect fundamental underlying cultural considerations about the roles of privacy and free expression more generally throughout society. Current interpretations of the European Union laws, in particular the recent Dutch court decision, suggest that in Europe, individuals will have more scope to seek to enforce subjective conceptions of privacy. In other words, individuals will have clearer avenues to subjectively say what they find offensive and should be removed in terms of their own lives and reputations. Whether they win or lose (or whether some individuals do not have the wherewithal to fight a battle in court), the existence of a more subjective individual privacy right in the European Union weighs in significant contrast to the position in the United States where privacy does not function significantly as an individual right.

Google and entities like it are now facing significant costs and uncertainties in terms of being cast into the position of responsibility in terms of implementing the right to be forgotten. They will have to shore up their own internal policy

guidelines in light of judicial decisions in the European Union as well as any information coming out of the Article 29 Working Party. They will also have to, and currently are, expending resources on training personnel to implement their policies, including handling large volumes of removal requests with respect to personal information. The need to employ and train sufficient personnel to deal individually with each removal request may simply not be viable for a number of online service providers. It may lead to a situation where such entities basically try to automate removal requests and err on the side of removal, or they may fail to implement any useful policies in the hope that the responsibility for making these determinations will ultimately be taken out of their hands and that national governments will develop more workable guidelines on the right to be forgotten.

CONCLUSION

Lamenting the bygone days of privacy, Chief Judge Kozinski once wrote:

> No matter how private, dangerous, hurtful, sensitive, or secret a piece of information may be, any fool with a computer and an internet connection—which means just about everybody—can post it online, never again to be private or secret. They say that removing something from the internet is about as easy as removing urine from a swimming pool, and that's pretty much the story.[140]

The EU's aggressively-evolving right to be forgotten upends this status quo in Europe-and has ramifications internationally. The lack of international harmonization on new digital privacy laws is perhaps now the least of worries for global online businesses. At present, their most significant struggle is determining how to implement the European right to be forgotten, at least with respect to European business operations, in light of the vagaries surrounding the current law as well as the fact that the current regulations are something of a moving target. Between the activities of the Article 29 Working Party and the forthcoming GDPR, global businesses know that the one constant in these regulations is change and that they will be expected to implement the changes in their internal policies as and when they come into being. In the interim, courts of the European Union will continue to interpret the current laws which may enhance certainty in some areas and may muddy the waters in others. For example, the recent Dutch decision gives online businesses some clarity as to how to treat information about serious criminal convictions, but at the same time adds a judicial gloss on the *Google Spain* precedent in terms of adding criteria relating to "irrelevant," "excessive," or "unnecessarily defamatory" information, which may or may not be followed by other European Union courts.

The upshot is that the implementation of the fundamental European Union right to be forgotten has effectively been placed in the hands of entities who are not well placed to maintain that responsibility. Entities like Google have neither the

[140] Alex Kozinski, *The Dead Past*, 64 STAN. L. REV. ONLINE 117, 124 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-117.pdf.

corporate interest nor the expertise to protect individual privacy in this way, particularly if they are being asked to implement different procedures in different jurisdictions. For example, search results in Europe now look significantly different to search results in the United States in terms of personal information. These entities will face increasing pressure to comply with removal requests in Europe with the threat of litigation for noncompliance looming, at least in relation to those with the wherewithal to bring legal action or to convince a government entity to pursue Google on their behalf.

The problem for online businesses is exacerbated by the fact that current regulations are disharmonized, lack clarity, and appear to be in a constant state of change. While we would prefer to conclude on a cheerier note, the best we can hope for is that the current international attention focused at this problem will lead to faster and clearer resolutions of some of the uncertainties about the nature of the right to be forgotten, its regulatory future, and the level of guidance or oversight that may be given to those businesses who are now required to implement it in practice on a daily basis. We hope that our observations in this Article may assist in outlining some of the key issues for those involved in law reform as well as those struggling to determine the appropriate boundaries of the right to be forgotten in business practice.

APPENDIX A

Article 17
Right to be forgotten and to erasure[141]

1. 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, especially in relation to personal data which are made available by the data subject while he or she was a child, 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.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) for reasons of public interest in the area of public health in accordance with Article 81;

---

[141] *GDPR*, *supra* note 14, art. 17.

(c) for historical, statistical and scientific research purposes in accordance with Article 83;

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;

(e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.