

Privacy, Speech, and the Digital Imagination

Specifying the value of privacy is notoriously difficult. We often resort to ideal concepts like “dignity” or “control” or “autonomy,” concepts that obscure as much as they reveal. At root this is because the value of privacy does not inhere in abstractions, but in lived experience. We enjoy the goods of privacy by participating in the forms of sociality that make these goods immanent (Post 1989, 9; Hirshleifer 1980, 649).

Forms of sociality lie at the intersection of the material and the imaginary. They exist as real social structures insofar as we share a commitment to their importance and worth (Searle 2006). These commitments in turn arise out of and are sustained by the fulfillment and nourishment we derive from the forms of life they inspire. This virtuous cycle is pervasive in ordinary life, but it is rare in the digital world. Virtual reality is evolving so rapidly that it lacks the settled forms of life necessary to underwrite shared commitments. It should come as no surprise, therefore, that our digital imagination has yet to settle on a coherent account of the value of privacy. The confusion is especially important when government seeks to restrain digital expression in order to protect the value of privacy.

That digital expression is somehow important to the traditional democratic value of freedom of speech is widely accepted. It is commonly agreed that “in light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an

important role in enhancing the public’s access to news and facilitating the dissemination of information in general.”¹ As the United States Supreme Court recently opined:

A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more. The Court has sought to protect the right to speak in this spatial context. A basic rule, for example, is that a street or a park is a quintessential forum for the exercise of First Amendment rights. . . . Even in the modern era, these places are still essential venues for public gatherings to celebrate some views, to protest others, or simply to learn and inquire.

While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the “vast democratic forums of the Internet” in general, . . . and social media in particular.²

At a minimum, the traditional democratic value of freedom of speech requires that digital expression should be curtailed only if necessary to achieve specific goods that we hold to be more important than the contribution of expression to the digital public sphere. If we wish to constrain expression to protect digital privacy, and if at the same time we have no very firm or clear conception of the nature of digital privacy, we face a serious challenge. The conundrum is unfortunately not theoretical, for we have recently witnessed powerful legal encroachments on communication that seem fundamentally confused in their apprehension of digital privacy.

I am referring to what has become known as the “right to be forgotten.” The right became internationally prominent in 2014 when the Court of Justice of the European Union (CJEU) decided the monumental case of *Google Spain SL v. Agencia Española de Protección de*

¹ Case of Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, ECtHR (Application no 22947/13) (February 2, 2016), at ¶ 56.

² *Packingham v. North Carolina*, 137 S.Ct. 1730, 1735 (2017).

Datos (“AEPD”) (“*Google Spain*”).³ *Google Spain* sought to interpret Directive 95/46/EC⁴ (“Directive”), which “is probably the most influential data privacy text in the world” (Kulk and Zuidvereen Borgesius, forthcoming, 14). The Directive contains comprehensive rules for processing the “personal data” of “data subjects”; it seeks to ensure that such personal data be used only for the “specified purposes”⁵ for which they have been properly acquired.⁶ The Directive protects what we may call “data privacy” by establishing “fair information practices” to assure the accuracy, transparency, and instrumental rationality of data processing (Flaherty 1986, 8). The point of these practices is to give data subjects “control,” or “informational self-determination,” over the use of their personal data.⁷

In essence, *Google Spain* held that the Google search engine (“Google”) processed personal data whenever it performed a search of internet sites for the name of a data subject. Applying the criteria of the Directive, the CJEU held that a data subject could ask Google to remove search results that produced personal data that were “inadequate, irrelevant or no longer

³ Case C-131/12 (May 13, 2014), available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

⁴ Directive 95/46/EC On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (October 24, 1995), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

⁵ See Article 8 of the Charter of Fundamental Rights of the European Union (“Protection of Personal Data”), Section 2, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>.

⁶ Directive, Article 6(1).

⁷ “Generally, the ‘privacy-as-control’ approach has manifested in the area of personal information protection as a call for awarding individuals the greatest control possible over their personal information. This is reflected in what are commonly referred to as Fair Information Practices.” (Levin and Abril 2009, 1009) (“The right to be forgotten represents ‘informational self-determination’ as well as the control-based definition of privacy and attempts to migrate personal information from a public sphere to a private sphere.”) (Leta Jones 2016, 94) . In this regard, the right to “control” the manipulation of existing personal data must be sharply distinguished from the right to prevent surveillance, which is the right to prevent the augmentation of existing personal data. See Richards, Neil M. “The Dangers of Surveillance.” *Harvard Law Review* 126, no. 7 (May 2014): 1934-965.

relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine.”⁸ *Google Spain* concluded that a data subject could “require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that . . . he wishes it to be ‘forgotten’ after a certain time.”⁹

Following *Google Spain*, the European Union doubled down on the right to be forgotten by enacting the General Data Protection Regulation (GDPR),¹⁰ which will become the law of all EU member states and which contains a right to be forgotten that will likely be interpreted in light of *Google Spain*.¹¹ The GDPR marks the legislative triumph of a distinctive EU variant of the right to be forgotten that can be expected massively to constrain the international digital public sphere of the Internet.

The tension between the right to be forgotten and digital freedom of speech is palpable. By the beginning of 2017, the *Google Spain* decision had required Google to process 703,910 requests to remove 1,948,737 URLs from its search engine; some 43.2% of these URLs were

⁸ *Google Spain* at ¶ 94.

⁹ *Google Spain*, ¶ 89.

¹⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. The GDPR is due to go into effect on May 25, 2018. It repeals the Directive. Article 17 of the GDPR, which is entitled “Right to Erasure (‘Right to be Forgotten’),” is an explicit gesture toward the holding of *Google Spain*.

¹¹ GDPR, Art. 17.

erased from searches made under the name of the person requesting removal.¹² In the past several years, the right to be forgotten has been asserted by a vicar who resigned after villagers accused him of standing naked at a vicarage window and swearing at children; by a doctor convicted of attempting to spike his pregnant mistress' drinks with drugs to cause a miscarriage of their son; and by a butcher convicted of blackmail for threatening to send his estranged wife's wealthy parents videos of her participating in group sex (Williams 2015). The right to be forgotten has even been asserted against articles about the right to be forgotten (Peguera 2015).

The Index on Censorship denounced *Google Spain* as “akin to marching into a library and forcing it to pulp books” (Index on Censorship 2014). The European Union Committee of the British House of Lords responded to *Google Spain* by concluding (in bold-faced type) that **“the ‘right to be forgotten’ . . . must go. It is misguided in principle and unworkable in practice.”**¹³ Jimmy Wales, the co-founder of Wikipedia, condemned the right to be forgotten as “deeply immoral” because “history is a human right” (Curtis and Philipson 2014). The American legal scholar Jeffrey Rosen has observed that *Google Spain* and the GDPR portend a “titanic clash” with American free-speech principles (Rosen 2012).

The clash between the right to be forgotten and freedom of expression ultimately derives from the fact that the latter presupposes a form of sociality that depends upon intersubjective communication between persons, whereas the right to be forgotten presupposes an instrumental

¹² <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en> (Visited on March 17, 2017). For examples of sites that Google has and has not removed in response to *Google Spain*, see <https://www.google.com/transparencyreport/removals/europeprivacy/>.

¹³ House of Lords, European Union Committee, 2nd Report of Session 2014-15, EU Data Protection law: a ‘right to be forgotten’?, (23 July 2014), available at <http://www.publications.parliament.uk/pa/ld201415/ldselect/lducom/40/40.pdf>.

form of sociality in which persons exist as abstract agents who control and manipulate compilations of data. The right to be forgotten protects the right of persons autonomously to control information that pertains to them; the right to freedom of expression protects forms of communication that transpire in a common and shared world.

Data privacy conceptualizes personal data as something which persons use by gathering, storing, accessing, combining, analyzing, transmitting or obliterating. Information is conceived as a kind of “thing” that is controlled by one agent or another. Fair information practices specify who can “own” personal data, as well as the purposes for such data can be used. Fair information practices create accountability procedures to ensure that personal data are used only to serve specified purposes. The point of data privacy is to endow data subjects with the appropriate level of control over the use of their personal data. It is irrelevant whether data subjects suffer material or psychological harm from failure to comply with fair information practices,¹⁴ because damage is conceptualized as losing control to which data subjects are otherwise entitled.

The Directive (and the GDPR) are quite ambitious. EU data privacy seeks to apply fair information practices to the “processing” of “personal data,” which is defined as all information “relating” to an identifiable person.¹⁵ There is no requirement that “personal data” be limited to private information or that it be limited to information that, if released, would be harmful to a

¹⁴ *Google Spain*, at ¶ 96. See The Advisory Council to Google on the Right to be Forgotten (February 6, 2015), available at <http://docs.dpaq.de/8527-report-of-the-advisory-committee-to-google-on-the-right-to-be-forgotten.pdf>, at 5 (“The right to object to and require cessation of the processing of data about himself or herself . . . exists regardless of whether the processing at issue causes harm or is prejudicial in some way to the data subject.”).

¹⁵ *Google Spain*, at ¶ 4. Directive, Article 2(a).

data subject.¹⁶ Taken literally, personal data seems to include even “very innocuous published information such as the name of an author coupled with a book title” (Erdos 2015, 122). The Directive defines “processing” in equally expansive terms, 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.”¹⁷ Under this definition, every transmission of information over the Internet constitutes the “processing” of data.¹⁸

In applying the right to be forgotten to Google, therefore, the CJEU asked whether Google’s processing of personal data was “inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine.”¹⁹ This question presupposes a social world in which persons use Google searches for specific purposes, and in which the necessity of such searches can be assessed by the criteria of instrumental reason. This world corresponds to the ways in which large corporations and organizations gather and use personal data. Large institutions acquire data in order to achieve specific ends— to allocate welfare benefits or to determine the creditworthiness of debtors or to increase the effectiveness of health care. In such situations, it may make perfect

¹⁶ *Google Spain*, at ¶ 96.

¹⁷ Directive, Article 2(b). The GDPR defines “processing” in virtually the same way. See GDPR, Article 4(2).

¹⁸ Reference to the CJEU for a preliminary ruling in the criminal proceedings against Bodil Lindqvist, Case C-101/01 (November 6, 2003) ¶ 27, available at <http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en>.

¹⁹ *Google Spain*, ¶ 94.

sense to restrict the manipulation of data to particular purposes and to maximize the control of data subjects over the use of their personal data.

Yet all would agree that there are vast stretches of life in which this kind of instrumental reason is out of place. Friendship is not instrumental, nor is love, nor is play, nor is much of common human expression. Suppose, for example, that I write a blog about your birthday party, which I have just attended. I am processing your personal data, but I am not doing it for “specific” purpose. I am most likely engaging in what Habermas might call communicative action, which is expression designed to co-ordinate and affirm social understandings with friends and readers (Habermas [1962] 1970).²⁰

Someone who would ask whether my processing personal data about your birthday party has become “irrelevant” or “excessive” with respect to the purposes of my blog shows that they do not understand the social practice of writing a blog. The personal data in my blog are not connected to the purpose for which I am writing the blog in the same way that a “means” is connected to an “end.” When fair information practices are applied to communications like my blog, they advance criteria for assessing the legitimacy of processing personal data that are literally unintelligible. The criteria presuppose forms of sociality that have nothing to do with the relevant form of life in which my blog participates.

The same is true of the virtual public sphere, which is also characterized by communicative action rather than instrumental reason. Persons express themselves in the public sphere in order to engage in a dialogue that they hope will forge shared values and commitments.

²⁰ See, e.g., (Habermas [1962] 1970, 81-122); (Habermas [1968] 1972)

The metaphor of “control” is incompatible with the intersubjective nature of this dialogue (Schwartz 100, 760–761). Consider public discussion of Hillary Clinton’s emails or of Donald Trump’s “university.” Although such discussions will include a great deal of “personal data,” it makes little sense to ask who “controls” those data. In matters of legitimate public concern, we wish to promote an ongoing public dialogue that involves a common search for meaning in light of shared facts. To assert individual agential “control” of these facts is to shut down the exchange. In the context of the virtual public sphere, information is a public good.

We protect communicative exchange within the public sphere in order to sustain democracy. We can roughly define democracy as “government by public opinion” (Schmitt [1928] 2008, 275). It is for this reason that democracy requires the freedom of speech necessary to form public opinion (Post 2012, 13–21). I use the term “public discourse” to refer to the set of communications constitutionally deemed necessary to form a democratic public opinion.²¹ Democracy presupposes that dialogue within public discourse is intersubjective rather than instrumental (Michelman 1988, 1526–27). Public conversation must be permitted to follow the free play of public interest and attention; it cannot be bureaucratically organized to achieve specific purposes.²² For this reason, information within public discourse is (typically) not

²¹ POST, *supra* note **Error! Bookmark not defined.**, at 15. In this chapter, I am *not* using the term “public discourse” to refer to those speech acts that in American constitutional law would create the value of democratic legitimation for individual human beings. *Compare* (Post 2014, 71–74)

²² For this reason, speech within managerial spaces is differently protected than speech within public discourse. *See* Post, Robert C. “Between Governance and Management: The History and Theory of the Public Forum.” *UCLA Law Review* 34 (1987): 1713. ; Post, Robert C. “Meiklejohn’s Mistake: Individual Autonomy and the Reform of Public Discourse.” *University of Colorado Law Review* 64 (1993): 1109.

“owned” by one person or another; it is a common good that facilitates communal communicative exchange.²³

Google is essential to the infrastructure that sustains the virtual public sphere. It connects persons who wish to communicate with each other. It creates a moving archive that corresponds to the Internet itself.²⁴ The purpose of such an archive is comparable to the purpose of traditional library archives, which are dedicated to providing “the public the means of acquiring information, knowledge, education, aesthetic experience, and entertainment” (Molz and Dain 1999). Such archives sustain “democratic” culture²⁵ by “recapturing and extending democratic processes and potential” through linking persons to “the public sphere” (Buschman 2003, 175; Billington 2015, 254). The “allure of the archives,” writes Arlette Farge, is the anticipation of a “roaming voyage through the words of others,” so that we might “enter into an unending conversation about humanity” and about “the debates that surround us” (Farge 2013, 123–4). When might it be said that the processing of personal data necessary to populate such archives is

²³ The law of intellectual property, of course, represents an awkward exception to this generalization.

²⁴ In *Case of Times Newspapers Ltd (nos 1 and 2) v. The United Kingdom*, Applications nos 3002/03 and 23676/03, ECtHR (October 6, 2009), the ECtHR acknowledged “the substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free. The Court therefore considers that, while the primary function of the press in a democracy is to act as a “public watchdog”, it has a valuable secondary role in maintaining and making available to the public archives containing news which has previously been reported.” *Id.* at ¶45, available at [http://hudoc.echr.coe.int/eng#{"dmdocnumber":\["848220"\],"itemid":\["001-91706"\]}](http://hudoc.echr.coe.int/eng#{).

²⁵ The 1979 White House Conference on Library and Information Services affirmed that “publicly-supported libraries are institutions of education for democratic living.” *Resolutions of the White House Conference on Library and Information Services 1979* 42 (March 1980).

“inadequate, irrelevant or no longer relevant, or excessive in relation to” this social purpose (Szekely 2014)?²⁶

There is no answer to this question. If we wish to use archives to produce shared understandings, we cannot accept the right to be forgotten, which is why even one of the GDPR’s most passionate advocates has observed:

The right to be forgotten is of course not an absolute right. There are cases where there is a legitimate and legally justified interest to keep data in a data base. The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a right of the total erasure of history (Reding 2012).

History is produced by a form of sociality that regards personal data as a communal good, rather than as a “thing” that is under the “control”²⁷ of any single data subject. Data privacy would unravel the fabric of history itself. It would authorize me to prevent you from narrating your account of historical events if it included information “relating to”²⁸ me, and vice versa. Yet history can be constructed only from the interplay of such perspectives, including the personal data contained within them. That is why “It is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of” past publications.²⁹

²⁶ For a fascinating if unsuccessful effort to wrestle with this question, Szekely, Ivan. 2014. “The Right to be Forgotten and the New Archival Paradigm.” Essay. In *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*, Alessia Ghezzi, Angela Guimares Pereira, and Lucia Vesnic-Alujevic 28–49.

²⁷ GDPR, recital 7.

²⁸ Directive, Article 2(a). Article GDPR, Article 4(1).

²⁹ *Węgrzynowski and Smolczewski v. Poland*, ECtHR (Application No. [33846/07](#)), July 16, 2013, at ¶ 65.

This same need for communal information applies when personal data are communicated in the public sphere, which is where our understandings of history are forged. Public discourse would collapse if individuals were authorized to withdraw from circulation all information “relating to” themselves.³⁰ The pressing importance of self-governance gives us good constitutional reasons to release public discourse from the grip of data privacy. Fair information practices would in effect cede power to create public opinion to those entitled to control the circulation of personal data in the public sphere.

This tension is so obvious that both the Directive and the GDPR acknowledge forms of public communication that should be exempt from the reach of data privacy.³¹ The Directive provides that “Member States shall provide for exemptions or derogations from the [Directive] for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”³² The GDPR more capaciously provides that “Member States shall by law reconcile the right to the protection of personal data pursuant to this

³⁰ See, e.g., *Dresbach v. Doubleday & Co., Inc.*, 518 F.Supp 1285, 1289-91 (D.C. 1981); *Bonome v. Kaysen*, 17 Mass. L. Rptr 695 (2004); *Anonsen v. Donahue*, 857 S.W.2d 700 (Tex Ct. App. 1993).

³¹ Both the Directive and GDPR also permit the processing of personal data that is used “purely” for personal or household activities. See Directive, Article 3(2), Recital 12; GDPR, Article Article 2(2)(c); Recital 18. But the dissemination of information to the general public through the internet is not considered a personal or household activity. See Opinion 5/2009 of the Article 29 Data Protection Working Party (*On Online Social Networking*) (June 12, 2009), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

³² Directive, Article 9. For an exhaustive and disquieting study of how the national law of EU member states seeks (or does not seek) to reconcile the Directive with journalistic freedom, see David Erdos, *European Union Data Protection Law and Media Expression: Fundamentally Off Balance*, 65 INT’L COMP. L. Q. 139 (2016); David Erdos, *European Regulatory Interpretation of the Interface between Data Protection and Journalistic Freedom: An Incomplete and Imperfect Balancing Act?* -- PUB. L. 631 (2016); David Erdos, *Statutory regulation of professional journalism under European data protection: down but not out?* 8 J. MEDIA L. 229 (2016).

Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.”³³

The important theoretical question, then, is how “freedom of expression and information”³⁴ can be *reconciled* with the regime of instrumental reason that structures data privacy. Neither the Directive nor the GDPR offers so much as a hint. When pressed, reconciliation is explained through the metaphor of striking “a balance between [data] privacy and freedom of expression.”³⁵ But it is hard to understand how the image of balancing makes sense when data privacy and freedom of expression presuppose mutually exclusive social domains. The possibility of public discourse is foreclosed if personal data must be processed according to the managerial logic of data privacy, but fair information practices are eliminated if public discourse is exempted from this logic to allow for the free play of common information. How data privacy might be safeguarded *within* public discourse is unexplained, because data privacy exists in a bureaucratic universe that is incompatible with the communicative action constitutive of the public sphere.

Within the world of print or broadcast media, very few would dare to claim that persons should have the right to “control” the dissemination of any information “relating” to them, however innocuous. The need for information as a public good, the necessity for common

³³ GDPR, Article 85(1).

³⁴ In the European context, the “right of . . . information” focuses on the right of the public to *receive* information. See Charter, Article 11, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN> (Italics added).

³⁵ WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, RECOMMENDATION 1/97: DATA PROTECTION LAW AND THE MEDIA (February 25, 1997), at 5, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf. See *Google Spain*, ¶81; Directive, Recital 37.

discussion, are just too obvious. But by creating the right to be forgotten, the CJEU seemingly accepts the validity of such a claim with respect to Google, even though Google plays as important a role in the virtual public sphere as do the print or broadcast media in the traditional public sphere.³⁶ How could the CJEU have made such a categorical mistake?

I suggest that the CJEU's confusion reflects our uncertainty in the face of digital social practices. In the traditional press, no one would think to categorize Beyoncé's birthday (September 4, 1981) as a "thing" that she can control. Yet if information identifying her birthday is collected in digital form, available for processing for various purposes, we may become unsure how to characterize it. We might well conclude that Beyoncé should be able to control the dissemination of her birthdate if it is stored within the data bank of a large organization to serve managerial purposes. In creating the right to be forgotten, the CJEU generalized from this intuition.

The fallacy of the CJEU was to focus on the digital form of information, rather than on the human relationships in which information is embedded. Information that is incorporated into managerial regimes ought to be regulated according to the technocratic logic of such domains. But information that is constitutive of communication action ought to be regulated in ways that are compatible with communicative action. It does not matter how information is stored, whether digitally or in print. What matters are the forms of sociality that we wish information to serve. It is possible that the CJEU failed to grasp this fundamental insight because it was blinded by

³⁶ See Post, Robert C. 2018. "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere." *Duke Law Journal*. doi:10.2139/ssrn.2953468.

Google's digital character. The CJEU seems to have imagined that the mere fact of digitization produces` its own form of sociality. But this is manifestly not the case.

Data privacy arose out of the need to control the large-scale accumulation of personal data by organizations that created intolerable imbalances of power and information. This implies that fair information practices can and should apply to the personal data that Google gathers on its customers to effect "massive online captures of everydayness," which Shoshana Zuboff has labelled "surveillance capitalism" (Constantiou and Kallinnikos 2015, 55; Zuboff 2015, 75).³⁷ Such personal data is gathered and used for instrumental purposes. But it also implies that data privacy principles should not be applied to the vast stretches of digital communication that have nothing to do with the bureaucratic accumulation and manipulation of data.

Ordinary Google searches, from the perspective of Google's customers, underwrite the structure of the virtual public sphere. They create a web of communications that connects us each to the other as we participate in a public conversation out of which public opinion emerges. "Google and similar search engines are . . . increasingly becoming our windows to the world" (de Mars and O'Callaghan 2016, 267). The spell of the digital blinded the CJEU to the vital distinction between these two distinct forms of sociality within which digital information is embedded.

³⁷ On Google's acquisition of data, see Jones, Elisabeth A., and Joseph W. Janes. "Anonymity in a World of Digital Books: Google Books, Privacy, and the Freedom to Read." *Policy & Internet* 2, no. 4 (2010): 42-74. doi:10.2202/1944-2866.1072.; Van der Sloot, Bart, and Frederik Zuiderveen Borenius. "Google and Personal Data Protection." In *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, by Aurelio Lopez-Taurrella, 75-112. 2012.

Does this imply that privacy cannot be protected within the virtual public sphere? Not at all. It implies that privacy should be protected in the virtual public sphere in the same way that it is protected within the traditional public sphere. For more than a century, legal systems around the world have imposed legal restrictions upon the press and media that protect privacy by seeking to preserve the dignity of persons rather than informational self-determination. Let us call the telos of such restrictions “dignitary privacy.” It is sometimes said that “two of the most prominent conceptions of privacy are the control-based and the dignitarian” (O’Callaghan, forthcoming,)³⁸

To various degrees in various countries, law has proscribed the dissemination within public discourse of “personal information which individuals can legitimately expect should not be published without their consent”³⁹ because it would damage their “honour” or “psychological or moral integrity”⁴⁰ or “prejudice” their “personal enjoyment of the right to respect for private life.”⁴¹ When communications disrespectfully dredge up old events that compromise the dignity of a person, a version of the right to be forgotten can exist within the framework of dignitary privacy.⁴²

³⁸ Patrick O’Callaghan, *The Chance ‘to Melt into the Shadows of Obscurity’*” *Developing a Right to be Forgotten in the United* , in *PRIVACY: CORE CONCEPTS AND CONTEMPORARY ISSUES* (A. Cudd & M. Navin eds. 2018) (Forthcoming), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3009254.

³⁹ *Case of Axel Springer AG v. Germany*, (7 February 2012) (Application no 39954/08), ¶ 83.

⁴⁰ *Case of A. v. Norway* (9 April 2009)) (Application no 28070/06), ¶ 63.

⁴¹ *Case of Axel Springer AG v. Germany*, (7 February 2012) (Application no 39954/08), ¶ 83.

⁴² See Werro, Franz. "The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash." *Haftungsrecht im dritten Millennium - Liability in the Third Millennium*, 2009, 285-300. doi:10.5771/9783845213859-285.

In the law of France, as well as that of “other European countries,”⁴³ the latter version of the right to be forgotten is known as “le Droit à l’Oubli,” which places “a time limit on the publication of information: the press . . . cannot continue to publicize matters that are no longer in the public interest” and that can “relentlessly harm” persons “beyond a period of newsworthy relevancy” (Mantelero 2013, 229; LoCascio 2015, 299).⁴⁴ American courts have also sought to protect dignitary privacy. They have asked whether particular communications have become so offensive as defined by “community mores” that they cause “humiliation and mortification”⁴⁵ and cannot be justified by “a legitimate interest or curiosity”⁴⁶ of the public.⁴⁷ This can include dredging up old and offensive information.⁴⁸

Almost all legal systems determine violations of dignitary privacy by balancing the “seriousness” of harms caused by a communication against the communication’s “contribution . .

⁴³ Mantelero, Alessandro. "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'." *Computer Law & Security Review* 29, no. 3 (2013): 229-35. doi:10.1016/j.clsr.2013.03.010.

⁴⁴“In Continental Europe, the right to be forgotten can be considered as being contained in the right of the personality, encompassing several elements such as dignity, honor, and the right to private life. Manifold terminologies are used in the context of the right of personality—mainly the right for the (moral and legal) integrity of a person not to be infringed and for a sphere of privacy to be maintained and distinguished” (Weber 2011)

⁴⁵ Pavesich v. New England Life Ins. Co. 50 S.E. 68, 79 (Ga. 1905). “There must . . . some reasonable and plausible ground for the existence of this mental distress and injury. It must not be the creation of mere caprice nor of pure fancy, nor the result of a supersensitive and morbid mental organization, dwelling with undue emphasis upon the exclusive and sacred character of this right of privacy. . . . [A] violation of a legal right must . . . be of such a nature as a reasonable man can see might and probably would cause mental distress and injury to any one possessed of ordinary feeling and intelligence.” Schuyler v. Curtis, 147 N.Y. 434, 448 (1895). For a discussion of the sociological interconnection between community mores and emotional damage, see Post, *supra* note **Error! Bookmark not defined.**

⁴⁶ Virgil v. Time, Inc., 527 F.2d 1122, 1131 (9th Cir. 1975), *cert. denied*, 425 U.S. 998 (1976).

⁴⁷ Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993). When the first *Restatement of Torts* recognized the tort of invasion of privacy in 1939, it explicitly observed that the protection of privacy must be “relative to the customs of the time and place and to the habits and occupation of the plaintiff.” RESTATEMENT (FIRST) OF TORTS, § 867, comment c (1939).

⁴⁸ See, e.g., Melvin v. Reid, 297 P. 91 (Cal. App. 1931); Briscoe v. Reader’s Digest Ass’n, 483 P.2d 34 (Cal. 1971).

. to a debate of general interest.”⁴⁹ Protections of data privacy cannot analogously weigh harm to personality against the legitimate interests of the public, because data privacy does not contain within it any analogous concept of harm to personality. It instead imagines persons as agents who control information. Within the context of dignitary privacy, by contrast, “harm” is determined on the premise that the well-being of persons depends upon compliance with intersubjective norms of respect, which are embodied by rules of civil communication.⁵⁰

Dignitary and data privacy differ in essential respects. Dignitary privacy does not focus on personal data *per se*, but instead seeks to ascertain whether specific communications are consistent with civility rules that reciprocally define both individual and community identity.⁵¹ It asks whether communications are *appropriate*, meaning in accordance with “finely calibrated systems of social norms, or rules . . . [that] define and sustain essential activities and key relationships and interests” (Nissenbaum 2010, 2–3). Communications that are sufficiently outrageous are conceived as damaging human personality.

If data privacy follows an instrumental logic of rationality, dignitary privacy follows a hermeneutic logic of social norms. Data privacy focuses on the manipulation of data; dignitary privacy focuses instead on acts of communication. Dignitary privacy protects the human personality understood as embedded in social norms; data privacy protects the capacity of

⁴⁹ *Case of Axel Springer AG v. Germany*, (7 February 2012) (Application no 39954/08), ¶¶ 83, 89, 90. Compare RESTATEMENT (SECOND) OF TORTS § 652D (1977):

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

- (a) would be highly offensive to a reasonable person, and
- (b) is not of legitimate concern to the public.

⁵⁰ See Post, *supra* note **Error! Bookmark not defined.**

⁵¹ See Post, *supra* note **Error! Bookmark not defined.**, at 978-87.

autonomous human agents to exercise control. Damage to personality, which is essential to dignitary privacy, is irrelevant to data privacy, which focuses purely on the scope of control. Dignitary privacy turns on the legitimate interests of the public, whereas the data privacy is indifferent to those interests.

Most importantly, data privacy presupposes a form of sociality that is fundamentally incompatible with the public discourse, whereas dignitary privacy does not. Freedom of speech is generally regarded as essential to democracy because it empowers persons to participate in the formation of public opinion and hence to experience the state as potentially responsive to them.⁵² But if public discourse becomes sufficiently abusive and alienating, persons are unlikely to experience it as a medium through which they might influence the construction of public opinion. In such circumstances, public discourse will no longer serve the purpose of democratic legitimation, and the democratic justification for freedom of speech will *pro tanto* diminish.

This creates what I have elsewhere called “the paradox of public discourse”: Although public discourse can sustain democratic legitimation only if it is conducted with a modicum of civility, the enforcement of civility restricts freedom of speech (Post 1990, 601, 640–44, 680–84). The existence of the paradox demonstrates that dignitary privacy can be compatible with the democratic function of public discourse in ways that data privacy cannot. The genuine conundrum of the paradox means that different legal systems can resolve the balance between freedom of expression and dignitary privacy in different ways.

⁵² POST, *supra* note 21, at 39-42.

The extreme cultural diversity of the United States makes American courts loathe to restrict public curiosity in the name of intersubjective norms.⁵³ American law characteristically regards “the interest of the public in the free dissemination of the truth and unimpeded access to news” as “so broad, so difficult to define and so dangerous to circumscribe,” that they “have been reluctant to make . . . factually accurate public disclosures tortious, except where the lack of any meritorious public interest in the disclosure is very clear and its offensiveness to ordinary sensibilities is equally clear.”⁵⁴ The suppression of public discourse in the interests of dignitary privacy is thus rare and plausible only in exceptionally outrageous cases as measured by the extraordinary offensiveness of a publication (Barbas 2010, 172–73).⁵⁵ In Europe, by contrast, courts are far less deferential to the curiosity of the public⁵⁶ and far more sympathetic to the authoritative enforcement of social norms considered indispensable to dignitary privacy.⁵⁷

⁵³ In a nation as diverse as the United States, “what is ‘private’ so as to make its publication offensive likely differs among communities, between generations, and among ethnic, religious, or other social groups, as well as among individuals. Likewise, one reader’s or viewer’s ‘news’ is another’s tedium or trivia.” *Anderson v. Fisher Broadcasting Companies*, 300 Or. 452, 661 (1986).

⁵⁴ *Jenkins v. Dell Pub. Co.*, 251 F.2d 447, 450 (3d Cir. 1958).

⁵⁵ See, Lima, Matthew Nussbaum. "Jury awards Hulk Hogan \$115 million as Gawker looks to appeal." POLITICO Media. March 18, 2016. <http://www.politico.com/media/story/2016/03/jury-awards-hulk-hogan-115-million-as-gawker-looks-to-appeal-004433>.

⁵⁶ See, e.g., *Alesy Ovchinnikov v. Russia*, No. 24061/04 ECtHR (December 16, 2010), at ¶ 50, available at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjK1Zq_gKnPAhUm5oMKHeA3BGwQFggcMAA&url=http%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D001-102322%26filename%3D001-102322.pdf&usq=AFQjCNFWIMDcEbeo7clqXiUMwpoghhqFgg; *Case of Hanover v. Germany*, ECtHR (Application no 59320/00) (24 June 2004), at ¶ 65; Spanish Supreme Court Judgment n. 545/2015, October 15, 2015, at ¶ 6.

⁵⁷ *Biriuk v. Lithuania*, App no 23373/03 ECtHR (November 25, 2008), at ¶ 38, available at http://en.tm.lt/dok/Biriuk_v_Lithuania.pdf; *Tammer v. Estonia*, App. no. [41205/98](http://www.echr.coe.int/ViewDoc.aspx?id=102322) (6 February 2001), at ¶¶ 64-69. On the confidence of European courts to balance dignity and privacy against freedom of speech, see Ronald J. Krotoszynski, Jr., *Reconciling Privacy and Speech in the Era of Big Data: A Comparative Analysis*, 56 WM. & MY. L. REV. 1279, 1314-26 (2015).

These differences result from distinctive historical traditions that have produced divergent forms of elite control over social norms, divergent needs to appeal to democratic legitimation to justify state action, divergent commitments to cultural individualism,⁵⁸ and so on. Such differences suggest that distinct legal systems can differently resolve the paradox of public discourse and yet nevertheless retain the benefits of democratic legitimation.⁵⁹ There is no possible way, however, to eliminate the incompatibility between data privacy and public discourse. The bureaucratic domain of data privacy is fundamentally irreconcilable with the shared and open communicative space required by public discourse.

The CJEU in *Google Spain* must ultimately have realized this fact. It is noteworthy that although the decision purports to apply the instrumental logic of the Directive, it nevertheless negotiates a series of murky legal maneuvers that seem to point to the conclusion that the right to be forgotten can be successfully asserted only if the “harm” to a data subject is balanced against the “interest of the general public.”⁶⁰ Yet this balance is the precise legal form assumed by protections for dignitary privacy, which weigh damage to personality (a concept that does not exist within data privacy) against the legitimate concerns of the public. But the CJEU reached this conclusion in such an obscure and labyrinthine way that it is hard to be confident what *Google Spain* actually means.

⁵⁸ See, Post, Robert C. "Cultural Heterogeneity and Law: Pornography, Blasphemy, and the First Amendment." *California Law Review* 76, no. 2 (1988): 297. doi:10.2307/3480615.

⁵⁹ See Post, Robert. "Hate Speech." In *Extreme Speech and Democracy*, by Ivan Hare and James Weinstein, 123. Oxford University Press, 2009.

⁶⁰ *Google Spain*, ¶¶ 81, 99; Post, *supra* note 36.

It is certain, however, that by focusing primarily on data privacy and the Directive, and by obscurely invoking considerations appropriate to dignitary privacy only when backed into a conceptual corner,⁶¹ the CJEU failed to articulate a sophisticated or even adequate account of how dignity might be weighed against the public's need to know. This failure might have been avoided had the CJEU not been so distracted by the digital nature of the information at issue. *Google Spain* illustrates how difficult it is for courts to grasp in the digital world the same forms of ordinary sociality that are so salient elsewhere in constitutional doctrine.

Perhaps the digital world is as yet too shapeless to sustain the creation of sound principles of jurisprudential order. The legal anthropologist Paul Bohannan once defined law as the "double institutionalization" of norms (Bohannan 1965, 35–36). Law functions well when it can take norms that society has already institutionalized and re-institutionalize them to serve the specific needs of the legal system. But if society lacks such norms, as seems to be the case within the digital world, legal regulation becomes destabilized and uncertain.⁶²

It is common ground, however, that in the context of regulating public discourse “[p]recision of regulation must be the touchstone in an area so closely touching our most precious freedoms.”⁶³ The consequences of conceptual confusion when the legitimacy of

⁶¹ The CJEU had access to those considerations insofar as Article 7 of the Charter, which provides that “[e]veryone has the right to respect for his or her private and family life, home and communications,” available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>, was also involved in the *Google Spain* case. Article 7 refers to dignitary privacy, *see* Post, *supra* note 36, and was specifically (if obscurely) mentioned by the CJEU in its *Google Spain* opinion as relevant to its decision. *Google Spain*, ¶ 99.

⁶² As Justice Harlan Fiske Stone once put it, “moral standards must become generally settled and accepted by society before they can find expression in law as an established rule of conduct. The moral rule must be a settled principle of social conduct before the law can or should attempt to make that principle mandatory upon all members of the community” (Stone 1915, 34).

⁶³ *NAACP v. Button*, 371 U.S. 415, 438 (1963).

democratic self-governance is itself at stake can be quite significant, as the example of *Google Spain* well illustrates. Certainly we owe it to ourselves to try to see more clearly into the digital abyss.

References

- Barbas, Samantha. 2010. "The Death of the Public Disclosure Tort: A Historical Perspective." *Yale Journal of Law and Humanities* 22 (171). doi:10.5040/9781474200974.ch-002.
- Bohannon, Paul. 2009. "The Differing Realms of the Law." *American Anthropologist* 67 (6): 33–42. doi:10.1525/aa.1965.67.6.02a00930.
- Buschman, John. 2003. *Dismantling the public sphere: situating and sustaining librarianship in the age of the new public philosophy*. Westport (Conn.): Libraries Unlimited.
- Constantiou, Ioanna D, and Jannis Kallinikos. 2014. "New games, new rules: big data and the changing context of strategy." *Journal of Information Technology* 30 (1): 44–57. doi:10.1057/jit.2014.17.
- Crawford, Alice, and James H. Billington. 2017. *The meaning of the library: a cultural history*. Princeton, NJ: Princeton University Press.
- Curtis, Sophie, and Alice Philipson. 2014. "Wikipedia founder: EU's Right to be Forgotten is 'deeply immoral'." *The Telegraph*. Telegraph Media Group. August 6. <http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html>. .
- Erdos, David. 2015. "From the Scylla of Restriction to the Charybdis of License? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection." *Common Market Law Review*, April, 119–54.
- Flaherty, David H. 1986. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology, & Human Values* 11 (1): 7–18. doi:10.1177/027046768601100102.
- Google. 2017. *Transparency Report*. Google. <https://www.google.com/transparencyreport/removals/europeprivacy.com/transparencyreport/removals/europeprivacy/>
- Habermas, Jürgen. 1971. *Toward a rational society: student protest, science, and politics*. Translated by Jeremy J. Shapiro. Boston: Beacon Press.
- _____. 1972. *Knowledge and Human Interests*. Translated by Jeremy J. Shapiro. Boston: Beacon Press.
- Hirshleifer, Jack. 1980. "Privacy: Its Origin, Function, and Future." *Journal of Legal Studies* 9 (4): 649–64.

- Index on Censorship. 2014. "Index blasts EU court ruling on "right to be forgotten ..."
Index on Censorship. May 13. indexoncensorship.org%2f2014%2f05%2findex-blasts-eu-court-ruling-right-forgotten%2f&p=DevEx,5063.1.
- Jones, Elisabeth A., and Joseph W. Janes. 2010. "Anonymity in a World of Digital Books: Google Books, Privacy, and the Freedom to Read." *Policy & Internet* 2 (4): 42–74. doi:10.2202/1944-2866.1072.
- Jones, Meg Leta. 2016. *Ctrl Z: the right to be forgotten*. New York: New York University Press.
- Kulk, Stefan, and Frederik Zuiderveen Borgesiu. 2017. "Privacy, freedom of expression, and right to be forgotten in Europe." Essay. In *Cambridge Handbook of Consumer Privacy*, edited by Jules Polonetsky, Omer Ten, and Evan Selinger.
- _____. 2015. "Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands After Google Spain." *European Data Protection Law Review* 1 (2): 113–24. doi:10.21552/edpl/2015/2/5.
- Levin, Avner, and Patricia Sánchez Abril. 2009. "Two Notions of Privacy Online." *Vanderbilt Journal of Entertainment & Technology Law* 11 (4): 1001–51.
- LoCascio, Steven M. 2015. "Forcing Europe to Wear Rose-Colored Google Glass: The "Right to be Forgotten" and the struggle to Manage Compliance Post Google Spain." *Columbia Journal of Transnational Law* 54 (1): 296.
- Mantelero, Alessandro. 2013. "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'." *Computer Law & Security Review* 29 (3): 229–35. doi:10.1016/j.clsr.2013.03.010.
- Michelman, Frank. 1988. "Law's Republic." *Yale Law Journal* 97: 1493.
- Molz, Redmond Kathleen, and Phyllis Dain. 2001. *Civic space/Cyberspace: the American public library in the information age*. Cambridge, MA: MIT Press
- Nussbaum, Matthew. 2016. "Jury awards Hulk Hogan \$115 million as Gawker looks to appeal." *POLITICO Media*. March 18. <http://www.politico.com/media/story/2016/03/jury-awards-hulk-hogan-115-million-as-gawker-looks-to-appeal-004433>.
- O' Callaghan, Patrick, and Sylvia. 2016. "Privacy and Search Engines: Forgetting or Contextualizing?" *Journal of Law and Society* 43 (2): 257–84. doi:10.1111/j.1467-6478.2016.00751.x.
- O'Callaghan, Patrick. 2018. "The Chance 'to Melt into the Shadows of Obscurity'." Essay. In *Privacy: Core Concepts and Contemporary Issues*.

- Peguera, Miquel. 2015. "No more right-to-Be-Forgotten for Mr. Costeja, says Spanish Data Protection Authority." *Center for Internet and Society*. Stanford University. October 3. <https://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority>.
- Post, Robert C. "Meiklejohn's Mistake: Individual Autonomy and the Reform of Public Discourse." 1993. *University of Colorado Law Review* 64: 1109.
- _____. 1987. "Between Governance and Management: The History and Theory of the Public Forum." *UCLA Law Review* 34: 1713.
- _____. 1988. "Cultural Heterogeneity and Law: Pornography, Blasphemy, and the First Amendment." *California Law Review* 76 (2): 297. doi:10.2307/3480615.
- _____. 1989. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77 (5): 957. doi:10.2307/3480641.
- _____. 2012. *Democracy, expertise, academic freedom: A First Amendment Jurisprudence for the Modern State*. New Haven, CT: Yale University Press.
- _____. 2016. *Citizens divided: campaign finance reform and the constitution*. Cambridge, MA: Harvard Univ Press.
- _____. 2009. "Hate Speech." Essay. In *Extreme Speech and Democracy*, by Ivan Hare, and James Weinstein 123. Oxford University Press.
- _____. 2014. *Citizens Divided: Campaign Finance Reform and the Constitution*. Harvard University Press.
- Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review* 126 (7): 1934–65.
- Rosen, Jeffrey. 2015. "The Right to Be Forgotten." *The Atlantic*. Atlantic Media Company. October 6. <http://www.theatlantic.com/magazine/archive/2012/07/the-right-to-be-forgotten/309044/>.
- Schmitt, Carl. 2008. *Constitutional Theory*. Translated by Jeffrey Seitzer. Durham, NC: Duke University Press.
- Schwartz, Paul M. 2000. "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices." *Wisconsin Law Review*, 743. doi:10.2139/ssrn.254849.
- Searle, John R. 2006. "Social Ontology: Some Basic Principles." *Revista de Sociologia* 80: 51–71. doi:10.5565/rev/papers/v80n0.1769.

Stone, Harlan Fiske. 1915. *Law and its Administration*. New York, NY: Columbia University Press.

van der Sloot, Bart, Frederik Zuiderveen Borenius, and Aurelio Lopez-Taurrella. 2012. "Google and Personal Data Protection." Essay. In *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, 75–112.

Weber, Rolf H. 2011. "The Right to Be Forgotten: More Than a Pandora's Box?" *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2: 120.

Werro, Franz. 2009. "The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash." *Haftungsrecht im dritten Millennium - Liability in the Third Millennium*, 285–300. doi:10.5771/9783845213859-285.