

The View from the Crossroads: The European Union’s New Data Rules and the Future of U.S. Privacy Law

Alessandra Suuberg*

We need a better, simpler narrative of U.S. privacy laws.

—Peter Fleischer,
Global Privacy Counsel for Google (2013)¹

You have zero privacy anyway. Get over it.

—Scott McNealy, Sun Microsystems (1999)²

I.	INTRODUCTION: E.U. DATA PROTECTION LAW GETS AN UPGRADE	268
II.	THE CONCEPTUAL DIVIDE	271
III.	DEFINING PRIVACY: UNDERSTANDING WHAT IS AT STAKE	275
	A. <i>Privacy vs. Data Protection</i>	275
	B. <i>Government Threats vs. Private Threats</i>	276
IV.	PROTECTING PRIVACY	277
	A. <i>Comprehensive vs. Sectoral</i>	277
	B. <i>Europe vs. America</i>	278
V.	THE END OF PRIVACY AS WE KNOW IT?	280
	A. <i>Law vs. Innovation</i>	281

* © 2013 Alessandra Suuberg. Senior Managing Editor, Volume 16, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2014, Tulane University Law School; A.B. 2011, Brown University. The author thanks all who contributed support, edits, perspective, and sources over the past year and the members of Volume 16 for their hard work this semester.

1. Peter Fleischer, *We Need a Better, Simpler Narrative of U.S. Privacy Laws*, PETER FLEISCHER: PRIVACY . . . ? (Mar. 12, 2013, 4:37 PM), <http://peterfleischer.blogspot.com/2013/03/we-need-better-simpler-narrative-of-us.html> (asserting that the United States has a robust legal framework for privacy, but needs to articulate it more effectively to the rest of the world). *But see* Liat Clark, *U.S. Privacy Advocates Head to Brussels in Show of Support*, WIRED.CO.UK (Jan. 22, 2013), <http://www.wired.co.uk/news/archive/2013-01/22/us-eu-data-protection-advocates> (“Unlike the U.S., Europe has a set of basic rules and institutions in place to protect individuals’ privacy, and is trying to update its existing rules and institutions for the digital age. The U.S. needs similar protections—a basic, overarching privacy law, and institutions with the teeth to enforce it.”).

2. *See* PCWorld Staff, *Private Lives? Not Ours!*, PCWORLD (Apr. 18, 2000, 12:00 AM), <http://www.pcworld.com/article/16331/article.html>; *see also* Helen S. Popkin, *Privacy Is Dead on Facebook. Get over It.*, TECHNICA ON NBCNEWS.COM (Jan. 13, 2010, 8:56 AM ET), http://www.nbcnews.com/id/34825225/ns/technology_and_science-tech_and_gadgets/.

B.	<i>The Right To Be Forgotten vs. The Right To Remember</i>	282
C.	<i>The Opt-Out Revolution vs. The End of Privacy</i>	284
VI.	YOU CAN'T KEEP THE TIDES FROM COMING IN.....	285

I. INTRODUCTION: E.U. DATA PROTECTION LAW GETS AN UPGRADE

This piece has been written and rewritten for more than 120 years.³

The impetus is usually some technological advance—instantaneous photographs,⁴ the Internet and the growth of e-commerce,⁵ Google, Facebook, the “Internet of Things”⁶—that allows us as a society to become more connected, more informed, and more watched, and causes us to consider all over again that “full protection in person and in property is a principle as old as the common law; but it [is] necessary from time to time to define anew the exact nature and extent of such protection.”⁷

This time, the impetus is a comprehensive reform of the European Union’s data protection rules—the product of more than two years’ discussions among various stakeholders and the public, and a framework that European officials originally hoped to have in place by spring of 2014.⁸ The proposed General Data Protection Regulation would replace

3. See, e.g., Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (referring to “instantaneous photographs and newspaper enterprise”); Connie Davis Powell, “*You Already Have Zero Privacy. Get over It!*” *Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146, 146-47 (2011) (describing privacy on social networks).

4. Warren & Brandeis, *supra* note 3, at 195.

5. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 718 (2001).

6. This refers to the linking of physical and virtual objects. Karen Eltis, *Breaking Through the “Tower of Babel”: A “Right To Be Forgotten” and How Trans-Systemic Thinking Can Help Reconceptualize Privacy Harm in the Age of Analytics*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 71 (2011). Consider, next, the potential use of commercial drones. Carl Franzen, *Privacy Laws Can’t Handle New Wave of Commercial Drones, Senate Hearing Concludes*, VERGE (Mar. 20, 2013, 04:40 PM), <http://www.theverge.com/2013/3/20/4127988/senate-worried-drones-for-commercial-police-violate-privacy>.

7. Warren & Brandeis, *supra* note 3, at 193.

8. See *Commission Proposes a Comprehensive Reform of the Data Protection Rules*, EUR. COMMISSION (Jan. 25, 2012), http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm; Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, (General Data Protection Regulation), COM (2012) II final (Jan. 25, 2012) [hereinafter Draft], available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; Natasha Singer, *An American Quilt of Privacy Laws*,

the 1995 E.U. Data Protection Directive (95/46/EC) (1995 Directive), which predated widespread use of the Internet, personal computers, and smartphones.⁹ The goal is a new two-part legal framework that addresses both the processing of personal data in criminal investigations and prosecutions, and consumer control over the way that Web sites and marketing companies surreptitiously collect information to “build profiles of people’s behaviors, browsing histories and shopping habits by tracking them online and off” in order to sell the information to marketers and others.¹⁰ Several proposals “go well beyond the voluntary [privacy] policies of companies like Google,” based in an American system that is less protective of personal data from a government regulation standpoint.¹¹

Following the receipt of more than 3000 amendments and revelations about the U.S. National Security Agency’s PRISM program,¹² the European Parliament’s Civil Liberties, Justice and Home Affairs (LIBE) Committee postponed and finally held a vote approving a final package of amendments on October 21, clearing the way for approval by Parliament and negotiations with national governments.¹³

In addition to reacting to changes in the way data is collected and used, the reforms are intended to unify privacy law in the E.U., because the original twenty-seven member states each implemented the 1995 Directive, binding on them only in ultimate effect, differently.¹⁴ While the Directive itself was twelve pages long, its implementation in Germany, for example, was sixty pages long.¹⁵ As E.U. Justice

Incomplete, N.Y. TIMES (Mar. 30, 2013), <http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html?pagewanted=all>.

9. See, e.g., *Controversy over EU Data Protection Reform*, DW (Mar. 5, 2013), <http://www.dw.de/controversy-over-eu-data-protection-reform/a-16647522>.

10. Editorial, *Europe Moves Ahead on Privacy*, N.Y. TIMES (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/opinion/europe-moves-ahead-on-privacy-laws.html?_r=0; see also Reidenberg, *supra* note 5, at 720-22; see Draft, *supra* note 8, at 1.

11. See, e.g., Editorial, *supra* note 10.

12. See European Pub. Health Alliance, *[Update] General Data Protection Regulation*, <http://www.epha.org/a/5801> (last visited Oct. 8, 2013).

13. Robert (Bob) Stankey, *Data Protection Regulation Proposal Approved by the European Parliament*, LEXOLOGY (Oct. 30, 2013), <http://www.lexology.com/library/detail.aspx?g=38c769f6-77d8-4e7d-b968-89cb242c6114>.

14. See Treaty on the Functioning of the European Union art. 288, Mar. 30, 2010, 2010 O.J. (C 83) 171, 172, available at <http://Eur-lex.Europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF> (explaining national authorities’ discretion with regard to directives); *Commission Proposes a Comprehensive Reform of the Data Protection Rules*, *supra* note 8.

15. *Reding Attacks ‘Scaremongering’ on Data Protection Shakeup*, THEPARLIAMENT.COM (Mar. 11, 2013), <http://www.theparliament.com/latest-news/article/newsarticle/reding-attacks-scaremongering-on-data-protection-shake-up/>.

Commissioner Viviane Reding explained this year at a cloud computing convention in Brussels, “Take those 60 pages and multiply by 27 member states, and you’ll get an idea of what the term ‘regulatory complexity’ means in practice.”¹⁶ Reding, who unveiled the new draft in 2012,¹⁷ said the goal was to replace that complexity with a single ninety-one-article law that covers all of Europe: “One continent, one law,” in the interest of simplicity and “opening a market.”¹⁸

Perhaps ironically, the proposal has elicited a negative reaction specifically from businesses. Last spring, during the long deliberations that characterize the European Union’s ordinary legislative procedure,¹⁹ American companies and the U.S. government lobbied heavily against the reforms in Brussels, where the European Parliament is based.²⁰ On one side, civil liberties groups such as the American Civil Liberties Union, the Consumer Federation of America, and the Friends of Privacy U.S.A. argued their case in support of tough restrictions on companies’ data practices, disagreeing with the lobbyists’ assertions that “consumer protections are as strong in the U.S. as in Europe.”²¹ On the other side, the U.S. Commerce Department lobbied on behalf of the Obama administration, expressing concerns about the impact on the American tech industry in Europe.²² Meanwhile, the U.S. Chamber of Commerce, Facebook, eBay, Amazon, and an industry group including Microsoft, Cisco, Intel, I.B.M., Oracle, Motorola Mobility, Texas Instruments, Dell,

16. *Id.*

17. Konrad Lischka & Christian Stöcker, *Data Protection: All You Need To Know About the EU Privacy Debate*, SPIEGEL ONLINE (Jan. 18, 2013, 10:15 AM), <http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html>.

18. *Reding Attacks ‘Scaremongering’ on Data Protection Shakeup*, *supra* note 15; see also Draft, *supra* note 8, at 2 (explaining “why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market”).

19. See TFEU art. 294.

20. This took place as the European Parliament worked out a draft regulation in preparation for negotiations with a council of twenty-seven European Union Justice Ministers. See Kevin J. O’Brien, *Silicon Valley Companies Lobbying Against Europe’s Privacy Proposals*, N.Y. TIMES (Jan. 25, 2013), http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html?_r=0; see also Lischka & Stöcker, *supra* note 17 (reporting that “the most extremist warnings . . . are coming out of the law firm Field Fisher Waterhouse,” where the head of the firm’s privacy and information law group said that “Gmail and Facebook may be forced to abandon their ad-supported models and start charging their customers in Europe or stop providing them with these popular services altogether”).

21. O’Brien, *supra* note 20.

22. *Id.*

and global tech companies have all contributed to an effort to weaken the proposed restrictions.²³

Neither the discussions of a trans-Atlantic privacy divide, nor the need to upgrade privacy law in light of new technologies, are new. Still, the amount of controversy surrounding the E.U. proposals suggests that we may be approaching a crossroads in privacy law in a few different regards.²⁴ This Comment aims to identify the points of divergence in how privacy has been understood and protected against private actors by these trading partners in the past and consider where data protection could be headed in the future on this side of the Atlantic.

This Comment, stated somewhere between serious and tongue-in-cheek, also aims to consider whether we might eventually stop writing about privacy law upgrades, stop fighting the tide of increasingly invasive technologies, accept that the idea of any kind of right to privacy is quickly becoming passé, and, to channel Scott McNealy, just “[g]et over it.”²⁵

II. THE CONCEPTUAL DIVIDE

Despite lacking a similar blanket data protection directive or the explicit constitutional protection of a fundamental privacy right,²⁶ the United States does not, to paint matters in broad strokes, simply value

23. *Id.*; Tom Brewster, *Facebook Lobbies Brussels in Earnest on EU Data Privacy Proposals*, TECHWEEK EUR. (Nov. 8, 2012), <http://www.techweekeurope.co.uk/news/facebook-lobbying-eu-data-privacy-98645>; see also Editorial, *supra* note 10. Bruce Swartz from the U.S. Department of Justice said the changes would make it more difficult to fight crime and pose a threat to security. Cameron Kerry from the U.S. Department of Commerce warned that the regulations would hurt the economy and cost jobs. *‘The Right To Be Forgotten’: U.S. Lobbyists Face Off with E.U. on Data Privacy Proposal*, SPIEGEL ONLINE (Ella Ornstein trans., Oct. 17, 2012, 11:29 AM), <http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html>. A document published by the U.S. Mission to the E.U. claimed that the proposed new regulation could “stifle innovation and inhibit growth.” Jennifer Baker, *Data Protection Overhaul [sic]*, NEWEUROPE ONLINE (Mar. 10, 2013, 7:09 PM), <http://www.neurope.eu/article/data-protection-overhall>.

24. The sense of having arrived at a crossroads has, moreover, been heightened by this year’s revelations of the extent of U.S. and U.K. intelligence agencies’ spying on U.S. and E.U. citizens. See, e.g., Laura Poitras, *Geheimdokumente: NSA horcht EU-Vertretungen mit Wanzen aus [Secret Documents: The NSA Listens in on E.U. Agencies with Bugging Devices]*, SPIEGEL ONLINE (June 29, 2013, 4:07 PM), <http://www.spiegel.de/netzwelt/netzpolitik/nsa-hat-wanzen-in-eu-gebaeuden-installiert-a-908515.html>; Glyn Moody, *Controversial EU Data Protection Regulation May Be Negotiated in Secret in Breach of Parliamentary Process*, TECHDIRT (June 3, 2013, 3:00 PM), <http://www.techdirt.com/articles/20130703/11301623706/snowden-effect-controversial-eu-data-protection-regulation-may-be-negotiated-secret-with-unknown-consequences.shtml>.

25. PCWorld Staff, *supra* note 2.

26. See Singer, *supra* note 8; Franz Werro, *The Right To Inform v. The Right To Be Forgotten: A Transatlantic Clash*, in LIABILITY IN THE THIRD MILLENNIUM 285, 292 (2009).

privacy less than Europe does.²⁷ For historical and cultural reasons, the concept has nonetheless evolved differently on either side of the Atlantic.²⁸

The underlying philosophical or conceptual difference can be described as one of privacy understood as dignity and informational self-determination versus privacy understood as liberty.²⁹ Whereas the core European privacy value is the right to control one's public image and honor, the core value in the United States is freedom from state encroachment,³⁰ or perhaps, bringing privacy torts aimed at private actors into the picture, the right "to be let alone."³¹

Privacy rights in the United States are derived from property rights and defined externally, rather than being inherently related to the person.³² So, if "[p]roperty grants an owner the exclusive right to dispose of what he owns," then in the American view "[p]rivacy is the exclusive right to dispose of access to one's proper (private) domain."³³ It goes along with this understanding that the essential American privacy standard is "expectation-driven" and "spatially-defined," and admittedly problematic in the digital context.³⁴

Meanwhile, to focus on the German example, the Federal Constitutional Court of Germany famously explained in its 1983 population census decision that informational self-determination guards the lines between the different contexts in an individual's life and thus is important for protecting freedom of speech and freedom of choice.³⁵ As

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

28. See *id.*

29. See *id.* at 1161. At the same time, the concept of informational self-determination that now is characteristic particularly of the German law was originally inspired in part by American writers. See Herbert Burkert, *Privacy—Data Protection: A German/European Perspective*, MAX PLANCK INST. FOR RES. ON COLLECTIVE GOODS, <http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf> (last visited Sept. 25, 2013).

30. See Whitman, *supra* note 27, at 1160-61.

31. Warren & Brandeis, *supra* note 3, at 193 (internal quotations omitted) (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888)). In tort law, the invasion-of-privacy torts, notably intrusion upon seclusion and publicity given to public life, address an intrusion into private affairs. See generally RESTATEMENT (SECOND) OF TORTS § 652 (1977).

32. This is generally true of the common law world. See Eltis, *supra* note 6, at 77.

33. *Id.* (citing Ernest van den Haag, *On Privacy*, in NOMOS XIII: PRIVACY 149, 150-51 (J. Roland Pennock & John W. Chapman eds., 1971)).

34. *Id.* at 76. Treating privacy like property may have made more sense in the past. The idea of a reasonable expectation of privacy translates awkwardly into the context of cyberspace, where there is no expectation that anything will be private. See *id.* at 78.

35. Gerritt Hornung & Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, 25 COMPUTER L. & SECURITY REV. 84, 85-86 (2009), available at <http://dx.doi.org/10.1016/j.ckr.2008.11.002>.

explained by Gerrit Hornung and Christoph Schnabel at the University of Kassel:

If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment . . . they may be inhibited in making use of their freedom. If citizens are unsure whether dissenting behaviour is noticed and information is being permanently stored, used and passed on, they will try to avoid dissenting behaviour so as not to attract attention.³⁶

The goal of European laws protecting informational self-determination, then, is twofold: to create a sphere for personal matters in which an individual can feel free from outside interference and to ensure citizens' unbiased participation in the political process.³⁷

Unlike property, the continental concepts of dignity and informational self-determination are not something that can be freely disposed of.³⁸ Therefore, it seems that European law helps the individual take an active role in controlling which information is known by which outside entity, whereas American law protects the comparatively passive individual from an active intruder (letting them choose whether or not to put up walls against the government or a private actor).

So, given these differing attitudes, whereas Americans are intuitively shocked to learn that Europeans tap phones up to 130-150 times more often than they do, European governments can dictate baby names, and public nudity is considered normal on the Continent; Europeans on the other hand are shocked by American practices regarding consumer data, workplace privacy, credit reporting, and discovery in litigation.³⁹

Moving past the conceptual underpinnings, in terms of the actual law's historical development on either side of the Atlantic, the United States is said to have ushered in the modern era of information privacy with Samuel Warren and Louis Brandeis's *The Right to Privacy* in 1890.⁴⁰ Troubled by the consequences of changes in the media and the advent of the camera, Warren and Brandeis argued in their seminal law review article for the existence of a common law right of privacy that allows an

36. *Id.* at 85.

37. *Id.* at 86.

38. See Whitman, *supra* note 27, at 1193. It is considered a fundamental human right. Julia Gladstone, *The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy*, 7 WILLAMETTE J. INT'L L. & DIS. RES. 10, 14 (2000).

39. Whitman, *supra* note 27, at 1156-59.

40. Warren & Brandeis, *supra* note 3; see also Gladstone, *supra* note 38, at 15; Robert P. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 135 (1996).

individual to choose the extent to which his thoughts and emotions are communicated to others.⁴¹ However, over time the principles they described were either “excised from the body of U.S. law on constitutional grounds, or . . . atrophied to the point of feebleness” on this side of the Atlantic.⁴²

Although the United States was generally seen as an early leader in information privacy protections, it lost that leadership position to Europe as the 1970s progressed and various states began enacting data protection legislation.⁴³ In 1970, the Hesse Act in Germany became the first data protection law introduced anywhere, inspired at least in part by concern about citizens and state power.⁴⁴ Data protection laws at the national level later came into force in Sweden and Denmark in the 1970s, followed by Norway and Finland in the 1980s.⁴⁵ In France, controversy over state data banks spurred the enactment of a similar law in 1978, a lead followed by Luxembourg, Belgium, Spain, and Portugal over the next two decades.⁴⁶ Finally, following the entry into force of the 1995 Directive, Italy and Greece transposed those rules into their own national laws.⁴⁷

Closer to home, the original American federal privacy statutes focused on regulating government intrusion; notably, the Privacy Act of 1974 and the Freedom of Information Act were spurred by the federal government’s accumulation of citizens’ personal information.⁴⁸ In contrast with their European counterparts, the American private-sector protections that developed over time were more decentralized, taking the form of industry-specific legislation, such as the Fair Credit Reporting Act, the Cable Communications Privacy Act, and the Video Privacy Protection Act of 1988, or voluntary guidelines such as the Direct Marketing Association’s privacy guidelines.⁴⁹

Finally, with regard to the present day, American privacy law in its current form has been summarized as a “patchwork” consisting of state

41. Robert Kirk Walker, *The Right To Be Forgotten*, 64 HASTINGS L.J. 257, 265 (2012).

42. *Id.*

43. Gellman, *supra* note 40, at 135; see also P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 L. & POL’Y INT’L BUS. 275, 278 (1998).

44. This was also due in part to a conflict between local communities and state administration over control of data after the introduction of large computing systems. Burkert, *supra* note 29, at 44-45.

45. *Id.* at 48.

46. The French administration came under fire for its secret SAFARI and GAMIN programs, which respectively maintained files on citizens and children’s health information. *Id.* at 49-50.

47. *Id.* at 51.

48. See Gladstone, *supra* note 38, at 15-16; see also Monahan, *supra* note 43, at 278.

49. See Monahan, *supra* note 43, at 280-82.

laws, federal sectoral laws, and other nonprivacy laws invoked in privacy matters.⁵⁰

III. DEFINING PRIVACY: UNDERSTANDING WHAT IS AT STAKE

Because “[t]here is no such thing as privacy as such,” there is no point to calling for privacy “as such.”⁵¹

One cannot talk about the best path forward without a grasp on what exactly needs to be protected and from whom. Understanding the divide between the United States and Europe over the General Data Protection Regulation requires that a few points be clarified: what data protection is and from where the perceived threats addressed by the new European legislation are coming.

A. *Privacy vs. Data Protection*

Not exactly preserving a right to be let alone, data protection in the European sense is “a type of privacy protection manifesting in special legal regulation [that] ensures a person the right of disposal over all data in connection with his personality,”⁵² and it is the specific focus of the 1995 Directive and the regulation intended to replace it in the European Union.

Throughout most of its history, the European model of data protection has included the data processing activities of the private sector.⁵³ The first generation of European data protection acts focused on state-run data controllers at a time when the developing social-welfare state required information on its citizens.⁵⁴ However, the second generation of European norms arose in the context of the aforementioned 1983 German Constitutional Court decision whose impact was felt in the Austrian, Norwegian, Finnish, Dutch, and Hungarian acts,⁵⁵ ensuring “specific rights for the individual concerning the whole process of

50. Fleischer, *supra* note 1.

51. Whitman, *supra* note 27, at 1221.

52. András Jóri, *1. Privacy and Privacy Protection*, DATAPROTECTION.EU (Jan. 16, 2007, 11:50 PM), <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy>.

53. Gladstone, *supra* note 38, at 16.

54. András Jóri, *3.1 First Generation Data Protection Norms*, DATAPROTECTION.EU (Jan. 9, 2007, 12:37 AM), <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.FirstGeneration> (“There was a threat that the state, by connecting various registries, would gain an informational superpower over the individual . . .”).

55. András Jóri, *3.2 The Census Decision and the Second Generation of Data Protection Norms*, DATAPROTECTION.EU (Feb. 2, 2007, 12:03 AM), <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.SecondGeneration> (“[B]asic right warrants . . . the capacity of the individual to determine in principle the disclosure and use of his/her personal data.” (footnote omitted)).

personal data processing.”⁵⁶ Typical attributes of the second-generation privacy legislation, which became more abstract and less technology-specific, included the right to object to data collection and the right to call for deletion of old information.⁵⁷

In the 1980s, as data protection laws proliferated across Europe, their harmonization became an important goal.⁵⁸ The 1995 Directive, which the proposed regulation now at issue would supersede, was an effort to provide adequate privacy protection across the European Union,⁵⁹ and it covered computerized and most manually processed data about natural persons.⁶⁰

B. *Government Threats vs. Private Threats*

As previously suggested, American privacy law generally considers the home the primary defense and the state the primary threat.⁶¹ American anxieties focus on the sanctity of the home, and the prime danger since the eighteenth century has been that the government will intrude there.⁶² Meanwhile, the fixation on intrusions by private actors such as the media is relatively lesser in the United States than it is in Europe.⁶³

Many of the famous American privacy cases have focused on these government intrusions,⁶⁴ and in them the citizen’s right to privacy has been found in the “penumbras” surrounding various amendments in the Bill of Rights:⁶⁵ the First Amendment protects freedom of association, the Third prevents the quartering of soldiers in private homes in times of peace, the Fourth prevents unreasonable searches and seizures, the Fifth prevents the government from forcing a citizen to speak to his own detriment, and the Ninth provides that the enumeration of certain rights

56. *Id.*

57. *Id.*

58. Reidenberg, *supra* note 5, at 731.

59. *Id.* at 732.

60. Gladstone, *supra* note 38, at 19. *See generally* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), *available at* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

61. Whitman, *supra* note 27, at 1215.

62. *Id.* at 1161-62.

63. *Id.* at 1162.

64. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012) (concerning unreasonable search and seizure and the Fourth Amendment); *Lawrence v. Texas*, 539 U.S. 558 (2003) (concerning sodomy laws and the Fourteenth Amendment).

65. *Griswold v. Connecticut*, 381 U.S. 479, 483-84 (1965).

in the Constitution “shall not be construed to deny or disparage others retained by the people.”⁶⁶

Meanwhile, the network of data protection law dealing with private entities at the federal level is notably inconsistent.⁶⁷ The private sector poses the newer threat,⁶⁸ and American policymakers have made relatively little progress so far in restricting these actors.⁶⁹ The American business lobby is strong,⁷⁰ and because the natural tendency with personal information is against transparency,⁷¹ with many businesses unwilling to be candid about their practices and give up these powerful, innovative tools,⁷² protection is limited.

In contrast, if Americans seem to think of privacy primarily as freedom from tyranny’s intrusion on a private space, then for Europeans to “be free” is not in the first instance to be free from government control, but to exercise free will—that is, to fully realize one’s own potential.⁷³ As a result, what we see once again with the proposed reforms in the European Union is that Europeans “trust the government more than the private sector with personal information,”⁷⁴ and as a partner in protecting their privacy.

IV. PROTECTING PRIVACY

A. *Comprehensive vs. Sectoral*

The European approach to privacy protection is comprehensive, meaning that it relies on “a broad scheme of strict privacy standards

66. See *id.* at 484.

67. Monahan, *supra* note 43, at 282.

68. *Id.*

69. See Editorial, *supra* note 10.

70. Monahan, *supra* note 43, at 280.

71. See Joel R. Reidenberg, *Restoring Americans’ Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 775 (1999); see also Paul Rose, *A Market Response to the European Union Directive on Privacy*, 4 UCLA J. INT’L L. & FOREIGN AFF. 445, 449 (2000) (citing Reidenberg, *supra*).

72. Rose, *supra* note 71, at 449-50.

73. Whitman, *supra* note 27, at 1181.

74. See *id.* at 1193 (citing Reidenberg, *supra* note 5, at 731); see also Whitman, *supra* note 27, at 1190 (“[T]raditional nineteenth-century values, with their honor-oriented, suspicious attitude toward the free press and the free market, have continued to make themselves felt . . .”). A similar preference for trusting government power over private power in Europe has been seen in the realm of Competition Law. See, e.g., Barry E. Hawk, *Giuliano Amato, Antitrust and the Bounds of Power*, 21 FORDHAM INT’L L.J. 1670, 1672 (1997) (“[I]n Europe there is still the tendency to prefer that government set the boundary between economic power and freedom of enterprises and not the constitutionally recognized solidity of specific freedoms of each and all. In contrast, the United States is more accepting of private power, continuing to see it as a natural manifestation or expression of private freedoms and thus preferred to the interventions of public power.”).

enforcement . . . which combines all aspects of privacy law across various industries under a single overarching regime.”⁷⁵

In contrast, the United States’ specific approach to data privacy and the private sector has generally been market-based and self-regulated at the federal level.⁷⁶ In the 1970s, the Privacy Act called for the formation of a Privacy Protection Study Commission to consider the need for additional legislation, including for the private sector.⁷⁷ In its report, the Commission concluded that voluntary guidelines and self-monitoring would be the better approach for the private sector.⁷⁸ As a result, no omnibus legislation governing private industry came to be.⁷⁹ Again in 1997, the White House in its policy plan for electronic commerce advocated for self-regulation and minimal government intervention, in keeping with the traditional U.S. view that “a complex legal or regulatory infrastructure [is] an undue restriction on the market.”⁸⁰

B. *Europe vs. America*

This brings us back to the discussion of the current E.U. proposals, around which the controversy and fervent lobbying seem to make the longstanding prediction come true: “For almost a decade, the United States and Europe have anticipated a clash over the protection of personal information.”⁸¹

In addition to lobbying by tech giants, the U.S. government was in direct contact with members of the European Commission as soon as proposals were drawn up in an effort to delay the reforms.⁸² Commentators have taken this strong interest from across the Atlantic as an indication that the European Union has become a world player in data

75. Kamaal Zaidi, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 MICH. ST. U. J. INT’L L. 169, 171 (2003).

76. David Raj Nijhawan, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939, 941 (2003).

77. Monahan, *supra* note 43, at 279.

78. *Id.* at 279-80.

79. *Id.* at 280.

80. *Id.* at 288.

81. Reidenberg, *supra* note 5, at 718. Note that this was written already in 1999, concerning the 1995 Directive. *Id.*

82. Tom Brewster, *E.U. Resists ‘Extreme’ U.S. Lobbying as Data Privacy War Brews*, TECHWEEK EUR. (Dec. 5, 2012), <http://www.techweekeurope.co.uk/news/EU-US-data-privacy-war-100999>.

protection regulation, and that “[w]hat Europe does will sooner or later be followed by other continents.”⁸³

The U.S. response to the 1995 Directive was embodied in the International Safe Harbor Privacy Principles, a move to resolve the major trade conflict that the new rules sparked by allowing U.S. companies to self-certify that they met an “adequacy” requirement for E.U. privacy protection.⁸⁴ At that time, the American business community had already put pressure on the Department of Commerce to block the comprehensive Directive.⁸⁵ Serving, in a sense, as a compromise, the Safe Harbor at least became a means of avoiding judgment on the status of American law or action under European law against U.S. companies.⁸⁶

With its first Directive, Brussels had essentially given an “ultimatum to Washington: adopt strong privacy laws, or stand the risk of losing countless trillions of dollars of business with Europe.”⁸⁷ Was the Safe Harbor a step in that direction?

It has been said that, with the 1995 Directive, Europe “displaced the role that the United States held since the famous Warren and Brandeis article in setting the global privacy agenda.”⁸⁸ Some have pointed after its passage to instances of U.S. legislators mimicking the 1995 Directive without considering the differences between the U.S. and E.U. legal systems, their different treatment of privacy, and the directive’s shortfalls.⁸⁹ Others claim that comprehensiveness is generally gaining momentum in the United States due to the combined influences of the Directive, the Safe Harbor, Congress’s increasing awareness that consumers need more privacy protections, increased protections by states, and concerns about U.S.-E.U. trade relations.⁹⁰

83. *Id.* Already in 1995, the European Union cast itself with its older data protection rules as “Privacy Cop [of the] World.” David Scheer, *Europe’s New High-Tech Role: Playing Privacy Cop to World*, WALL ST. J. (Oct. 10, 2003), <http://online.wsj.com/article/SB106574949477122300.html>. Some U.S. companies reacted to the 1995 Directive by adjusting their behavior to be compliant. Zaidi, *supra* note 75, at 175.

84. Whitman, *supra* note 27, at 1156; *U.S.-EU Safe Harbor Overview*, EXPORT.GOV (Jul. 1, 2013, 8:51 AM), http://export.gov/safeharbor/eu/eg_main_018476.asp.

85. Reidenberg, *supra* note 5, at 739-40.

86. *Id.* at 740.

87. Zaidi, *supra* note 75, at 175 (citing John R. Vacca, *The European Data Protection Directive: A Roadblock to International Trade?*, in *THE PRIVACY PAPERS* 569, 570 (Rebecca Herold ed., 2002)).

88. Reidenberg, *supra* note 5, at 737.

89. Angela Vitale, *The E.U. Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT’L L. 321, 321 (2002).

90. Zaidi, *supra* note 75, at 170.

However, if it is true that the United States will ultimately follow Europe's lead on data protection, then what is to be said for past failures to bring more dignity-based or comprehensive notions into the U.S. legal system,⁹¹ or for the fact that language has been adopted into the new set of E.U. reforms, word-for-word, from the American lobbyists?⁹² Privacy advocates were up in arms in February when the European Parliament decided to adopt a drafted opinion on data protection that they said watered down Justice Commissioner Viviane Reding's proposed rewrite.⁹³ Pro-privacy lobbyists from the European Digital Rights Group said the development would "rip up decades of European privacy legislation,"⁹⁴ and commentators have expressed concern that "measures designed to protect the European public are being stripped out and/or watered down by the very people . . . elected to defend [them]."⁹⁵

V. THE END OF PRIVACY AS WE KNOW IT?

On the topic of crossroads and choices, three especially provocative 'either-or's emerge for American observers from the controversy over the proposed regulation: First, should the law or the market most properly be looking after privacy moving forward, recognizing the significant intrusions by private actors into private lives; second, should the balance be struck on the side of dignity or expression when it comes to the proposed right to be forgotten; and third, what could the future ultimately

91. See, e.g., Whitman, *supra* note 27, at 1204 ("[I]t is best to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant.").

92. See, e.g., Tom Brewster, *Yahoo E.U. Data Privacy Lobbying Efforts Leaked*, TECHWEEK EUR. (Feb. 20, 2013), <http://www.techweekeurope.co.uk/news/yahoo-europe-data-privacy-lobbying-108089>; Baker, *supra* note 23 ("The LobbyPlag.eu website compares amendments put forward by MEPs with the text submitted by lobbyists for Amazon, Ebay and the American Chamber of Commerce. Civil liberties activists are angry that elected parliamentarians seem to have copied many amendments from these submissions.").

93. Kelly Fiveash, *Privacy Warriors Slam MEPs over 'Corporate-Friendly' Data Law Rewrite*, REGISTER (Feb. 22, 2013, 13:39 GMT), http://www.theregister.co.uk/2013/02/22/european_parliament_industry_committee_data_protection_amendments/.

94. *Id.*

95. Glyn Moody, *E.U. Data Protection: Proposed Amendments Written by U.S. Lobbyists*, COMPUTERWORLD UK (Feb. 11, 2013, 12:06), <http://blogs.computerworlduk.com/open-enterprise/2013/02/eu-data-protection-proposed-amendments-written-by-us-lobbyists/index.htm> (comparing original language—"Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour"—with a rewrite based on input from the American Chamber of Commerce—"A data subject shall not be subject to a decision which is unfair or discriminatory, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this data subject").

hold for the way that Americans think of privacy law, conceptually? Is the United States going to move toward adopting the Europeans' understanding of privacy as dignity and self-determination, and will citizens call for legislation that gives them more control of their data? Or will privacy become passé in a future in which they voluntarily cede, in the interest of convenience and connectedness, the expectation that they can ever, anywhere, truly be "let alone?"

A. *Law vs. Innovation*

One of the arguments against a comprehensive regime for privacy protection in the United States might be what has been dubbed "Grove's Law of Government," an observation about the disconnect between Washington and Silicon Valley.⁹⁶ In the words of Google CEO Eric Schmidt: "High tech runs three times faster than normal businesses. And the government runs three times slower than normal businesses. So we have a nine-times gap," and the only way to fix the problem is "to make sure that the government does not get in the way and slow things down."⁹⁷ According to Schmidt, regulation, which by its nature defines a path to follow, hinders real innovation.⁹⁸ Given that observation, is more comprehensive regulation actually going to be workable in the future, considering both the tension with innovation, as well as the significant influence of companies that have a reason to oppose it?⁹⁹

Scholarship has nonetheless suggested that the kind of self-regulation largely relied on in the United States will not be enough moving forward because it tends to be "more public relations than meaningful information privacy for citizens."¹⁰⁰ In the words of Joel Reidenberg, "[D]emocratic societies do not . . . typically sell off the political rights of citizens," and furthermore the privacy policies currently relied on by citizens to protect their rights are so convoluted that they require a college-level education to comprehend.¹⁰¹ Consent, without a clear understanding of its object, seems meaningless.

96. L. Gordon Crovitz, *Google Speaks Truth to Power*, WALL ST. J. (Oct. 24, 2011), <http://online.wsj.com/article/SB10001424052970204618704576645353164833940.html>.

97. *Id.*

98. *Id.*

99. See, e.g., Kelly Fiveash, *Does the Existence of Facebook Really Merit a Rewrite of Data Law?*, REGISTER (June 20, 2012, 08:58 GMT), http://www.theregister.co.uk/2012/06/20/data_protection_the_facebook_effect/ ("[Facebook's Mark] Zuckerberg has previously floated the smug notion that his userbase could be considered the world's third largest country."); Reidenberg, *supra* note 5, at 729 ("Technologies are not policy neutral. Technical decisions make privacy rules.").

100. Reidenberg, *supra* note 5, at 726.

101. *Id.* at 727.

B. The Right To Be Forgotten vs. The Right To Remember

It has been said that the differences between European and American thinking on privacy are most striking where free expression is involved.¹⁰² This is now playing out in American firms' and the U.S. government's concerns about the so-called "right to be forgotten," which has been among the new fundamental rights considered by the European Union.¹⁰³

The "faddish" proposal to allow individuals to call for the full erasure of their data once it is no longer needed for its original purpose could be a backlash against anachronistic U.S. approaches to privacy protection.¹⁰⁴ It also exemplifies the civilian attitude that control over personal information is essential to the "free unfolding of personality."¹⁰⁵

While it may not be entirely clear how the right to be forgotten differs from the right to erasure that already exists in the European Union's 1995 Directive,¹⁰⁶ a similar idea is not part of the American tradition:

The media and the press in particular have the constitutional right to publicize information as long as it is legally available The notion that privacy would put a limit on the right of the press to reveal the shameful past of an individual has been litigated and rejected in the Supreme Court of the United States. The notion that constitutional rights could be balanced against each other and that the freedom to speak and inform could be balanced against a competing constitutional right to one's private life does not seem to be an option under U.S. constitutional law.¹⁰⁷

102. Whitman, *supra* note 27, at 1196; *see also* Werro, *supra* note 26, at 286 ("The two Western cultures seem [to be] on irreconcilable paths when it comes to the recognition and enforcement of a right to be forgotten.").

103. Brewster, *supra* note 82; *see also* Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, 11 PVL R 06, Feb. 6, 2012, available at http://www.ico.org.uk/news/events/~media/documents/future_of_dp_in_europe_2012/ico_event_future_of_dp_in_europe_2012_Chris_Kuner_article.ashx.

104. Eltis, *supra* note 6, at 84; *see* Steven C. Bennett, *The "Right To Be Forgotten": Reconciling E.U. and U.S. Perspectives*, 30 BERKELEY J. INT'L L. 161 (2012) (explaining the right to be forgotten). Amended during the interservice consultation, the original plan would have made data controllers responsible for the ensured erasure of every Internet link or copy of the information; instead, now, it gives them a limited duty to inform third parties that the subject has requested erasure. Kuner, *supra* note 103, at 6.

105. Eltis, *supra* note 6, at 91 (footnote omitted).

106. Kuner, *supra* note 103, at 6.

107. Werro, *supra* note 26, at 286.

Freedom of expression is a value of constitutional magnitude in the United States, whereas protection of personal honor is not, so freedom of expression generally prevails on this side of the Atlantic.¹⁰⁸

However, arguments do undeniably exist for this kind of right in the United States:

There is a long list of people who clearly do [need a right to be forgotten], though, including: people who've escaped abusive relationships, people with marginalized religious or sexual preferences, people who fear losing their jobs or who've been pushed around by bullies throughout their lives. That list adds up to a very large portion of the world, in fact. The group of Ivy League elites who run Facebook might think there's no reason to be able to control access to their personal information, but many of them are less socially vulnerable and have less need to control their personal information.¹⁰⁹

The United States does value second chances, and it is possible that, without some kind of right to forget, the very American concept of reinventing oneself will be compromised.¹¹⁰

However, strong counterarguments cite freedom of expression, integrity of the record, and access to information.¹¹¹ According to Peter Fleischer, Google's Global Privacy Counsel, the right is a justification for online censorship,¹¹² and dignity-based privacy laws arguably do make each individual a censor of their own record. Meanwhile, Facebook's director of public policy in the United Kingdom and Ireland, Simon Milner, has said the right to be forgotten "raises many concerns with

108. Whitman, *supra* note 27, at 1196.

109. Marshall Kirkpatrick, *Why Facebook Is Wrong: Privacy Is Still Important*, READWRITE (Jan. 11, 2010), http://readwrite.com/2010/01/11/why_facebook_is_wrong_about_privacy; see also Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1532 (2012) (citing the paradigmatic example of Stacy Snyder, whose career was ruined by an unwise photo posting).

110. Eltis, *supra* note 6, at 88.

111. *Id.* at 84; see also Martin Bryant, *Online Privacy: Do We Have a Right To Be Forgotten? Should We 'Embrace Solitude?'*, NEXT WEB (Jan. 23, 2012), <http://thenextweb.com/socialmedia/2012/01/23/online-privacy-do-we-have-a-right-to-be-forgotten-should-we-embrace-solitude/>; 'The Right To Be Forgotten': U.S. Lobbyists Face Off with E.U. on Data Privacy Proposal, *supra* note 23 ("For the companies, it's not about freedom of speech, but about a brutal economic confrontation," says Jan Philipp Albrecht, a member of the European Parliament and the German Green Party's specialist there on data protection issues. "American companies' dominance of the Internet is especially at stake."); Whitman, *supra* note 27, at 1209 ("Freedom of expression has long been the most deadly enemy of continental-style privacy in America [It's] the values of Jefferson [vs.] the values of Goethe.").

112. 'The Right To Be Forgotten': U.S. Lobbyists Face Off with E.U. on Data Privacy Proposal, *supra* note 23.

regard to the right of others to remember,”¹¹³ perhaps understandable as an aspect of freedom of expression.

The right also faces the potential hurdle on a practical level that the kind of comprehensive erasure called for simply might not be feasible for services like Facebook, and so it would essentially have to change how the Internet works.¹¹⁴

C. *The Opt-Out Revolution vs. The End of Privacy*

On this side of the Atlantic, Facebook cofounder and CEO Mark Zuckerberg has said that, if he could do it all over again, all information on the social networking site would be public by default, claiming that this is just the way the social norm has evolved.¹¹⁵

Taking that into account, is it possible that the American public will essentially demand 24/7 surveillance, eventually?¹¹⁶ And if privacy is defined in terms of reasonable expectations of seclusion, then will “the sphere in which one can reasonably claim ‘solitude’ . . . contract” to the point where it is negligible?¹¹⁷ As put recently by Karen Eltis at the University of Ottawa, “Paradoxically, the more we are watched, the less privacy we expect . . .”¹¹⁸

At the same time, others point out that the demand for privacy protection against private data collectors is still growing.¹¹⁹ A recent study by market researcher Ovum suggests that people could even start going “data dark” in the next few years due to privacy concerns.¹²⁰ Only 14% of respondents reported trusting what Internet businesses claimed about uses of personal data, and 68% responded that they would block all

113. Milner also pointed out that, technically, the idea is unrealistic. Natasha Lomas, *Facebook Is in Europe Lobbying Against Unreasonable and Unrealistic Reform*, TECHCRUNCH (Nov. 9, 2012), <http://techcrunch.com/2012/11/09/facebook-lobbying-europe-on-unreasonable-and-unrealistic-privacy-law-reform-but-ec-commissioner-doesnt-sound-like-shes-for-turning/>.

114. *Id.* It is practically impossible to delete information that has been copied to other sites across the Internet. Tom Brewster, *Facebook: E.U.’s ‘Right To Be Forgotten’ Will Enforce More User Tracking*, TECHWEEK EUR. (Dec. 6, 2012), <http://www.techweekeurope.co.uk/news/facebook-europe-right-to-be-forgotten-tracking-101253>.

115. Marshall Kirkpatrick, *Facebook’s Zuckerberg Says the Age of Privacy Is Over*, READWRITE (Jan. 9, 2010), http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov (“I don’t buy Zuckerberg’s argument that Facebook is now only reflecting the changes that society is undergoing. I think Facebook itself is a major agent of social change and by acting otherwise Zuckerberg is being arrogant and condescending.”).

116. *See, e.g.*, Rosen, *supra* note 109, at 1529.

117. Eltis, *supra* note 6, at 80.

118. *Id.*

119. Monahan, *supra* note 43, at 283.

120. Antone Gonsalves, *Online Privacy: The Opt-Out Revolution Is Almost Here*, READWRITE (Feb. 12, 2013), <http://readwrite.com/2013/02/12/online-privacy-the-opt-out-revolution-is-almost-here>.

tracking, given the option.¹²¹ Furthermore, a 2010 survey conducted by researchers at the University of California at Berkeley reported that nine in ten people ages eighteen-to-twenty-four years and forty-five-to-fifty-four years would support a law requiring deletion of all stored data on request.¹²²

VI. YOU CAN'T KEEP THE TIDES FROM COMING IN

It seems, ultimately, that Europe and the United States are trying to achieve the same objectives, protecting a nebulous, intuitively important physical and psychological freedom enjoyed by their citizens, but with the key differences perhaps being that the United States prioritizes access to information and Europe prioritizes informational self-determination, and Europe has tended to favor omnibus legislation while the United States has always preferred self-regulation.¹²³

Will a convergence of views be inevitable,¹²⁴ given the degree of global interconnectedness and the routineness and value of trans-Atlantic business; will it mimic the international standardization of intellectual property laws, which also deal with intangibles and are important to trade; and will it mean that the United States eventually needs to follow Europe and abandon its sectoral approach in favor of a more comprehensive one?¹²⁵ Failing to do so, some say it could risk an ironic hindrance of innovation if privacy becomes too uncertain:

Unable to assess the risks of sharing, we might simply stop doing so. . . . A reliable and valid stream of intent and preferences is the lifeblood of . . . internet economy firms. . . .

. . . .

Without these limits, we might instead shift towards posting only content we feel is safe for a broad audience It would just create another digital town square—not a digital living room—tragically devoid of those little slivers of our everyday lives that represent who we are and make Facebook so unique.

Giving users complete control over their pasts might be the only way that Facebook continues to see—and mine—their futures.¹²⁶

121. *Id.*

122. *Id.*

123. Monahan, *supra* note 43, at 293.

124. Bennett, *supra* note 104, at 193.

125. Monahan, *supra* note 43, at 277-78.

126. Arun Sundararajan, *With Graph Search, It's Facebook vs. Facebook*, WIRED (Mar. 15, 2013, 2:30 PM), <http://www.wired.com/opinion/2013/03/dont-dismiss-facebook-graph-search-yet/>. However, recall that a similar argument was made in favor of the Online Personal Privacy

Just as the United States could find itself following Europe's comprehensive lead in the future, a European understanding of privacy as inherent dignity, rather than a disposable personal sphere, might be a better fit for a reality in which there is no real choice but to dispose of that sphere entirely. The notion of seclusion may be outdated once and for all, but there may still be a right to define and look after one's identity and dignity autonomously, nonetheless.¹²⁷

At any rate, it seems that the age of privacy as we knew it in the time of Warren, Brandeis, and their *Right to Privacy*—one still characterized by secluded spaces in which we can reasonably expect to be let alone—will soon be over. To quote New York City Mayor Michael Bloomberg in a recent interview on the topic of unmanned surveillance drones in the city, a topic that still feels like it belongs in the realm of science fiction, “You can't keep the tides from coming in.”¹²⁸

Europe seems to appreciate the inevitable, forward march of technology and to be working to keep its laws in step, and the American tech companies lobbying against its proposals probably understand it better than anyone. Taking that into account, maybe the most essential tension in data privacy is not actually shaping up to be between the European and the U.S. systems with their different notions of privacy, but between lagging, encumbered governments and the private-sector innovators they have to try to keep in check. Both have a significant influence on citizen's lives—and on each other.

But elaborating further on the tension between law and innovation brings us down an even more obscure path that would be difficult to navigate.

Act in 2002, the legislation failed, but the Internet thrived. See, e.g., S. 2201, *Online Personal Privacy Act: Hearing Before the Comm. on Commerce, Sci. & Transp.*, 107th Cong. 1 (2002).

127. Eltis, *supra* note 6, at 95.

128. David Pierce, *Mayor Bloomberg Says Surveillance Drones Are Inevitable in NYC: 'Get Used to It'*, VERGE (Mar. 24, 2013, 12:02pm), <http://www.theverge.com/2013/3/24/4141526/mayor-bloomberg-says-surveillance-drones-inevitable-in-nyc/in/3759737>.