University of Colorado Law Review

Volume 90 | Issue 2 Article 8

Spring 2019

Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure

Alexander Tsesis...

DATA SUBJECTS' PRIVACY RIGHTS: REGULATION OF PERSONAL DATA RETENTION AND ERASURE

ALEXANDER TSESIS*

The European Union's right to erasure came into effect May 25, 2018, as Article 17 of the General Data Protection Regulation ("GDPR").[1] Unlike the U.S. "marketplace of ideas" model of free speech,[2] the GDPR gives greater weight to data subjects' privacy interests than to audiences' curiosity about others' intimate lives. The U.S. and EU models advance human thirst for knowledge through open and uninhibited debates, whereas the internet marketplace tends to favor social media companies' commercial interests: put more specifically, free speech is not entirely harmonious with the interests of social media intermediaries whose algorithms tend to favor companies' bottom lines rather than strictly the expansion of knowledge.

European law is less tolerant of privacy invasions than is U.S. constitutional jurisprudence. The GDPR prohibits commercial digital entities from disseminating more information to third-party listeners than is necessary for carrying out a transaction. This regulatory scheme aims to balance the confli-

---

* Raymond & Mary Simon Chair in Constitutional Law and Professor of Law, Loyola University Chicago School of Law.

1. Commission Regulation 2016/679, art. 17, 2016 O.J. (L 119) 1, 4, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/9QUL-6Y84] [hereinafter GDPR].

2. Justice Oliver Wendell Holmes first developed the marketplace of ideas doctrine in a dissent:

> [M]en . . . may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution.

Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting). For an extended critique of the doctrine, see Alexander Tsesis, *Free Speech Constitutionalism*, 2015 U. ILL. L. REV. 1015, 1038–42.

cting interests of speakers[3] who post information online, and digital listeners, whose ranks extend well beyond the original data receiver to third-party consumer entities and private audiences. The GDPR limits the duration of time for which commercial audiences can retain personally identifiable information.[4] The law is a component of EU policies meant to limit commercial audiences' abilities to resend, sell, or share private information. Thereby, Europe aims to better safeguard data subjects' personal autonomy and dignity.[5] Its privacy protections contrast significantly from U.S. libertarian conceptions of the internet, which tend to favor business interests over consumer interests.[6]

---

3. Similar terminology can be found in Supreme Court jurisprudence. *See, e.g.*, Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 473 (2010) (Stevens, J., concurring in part and dissenting in part) ("The majority seems oblivious to the simple truth that laws such as § 203 do not merely pit the anticorruption interest against the First Amendment, but also pit competing First Amendment values against each other. There are, to be sure, serious concerns with any effort to balance the First Amendment rights of speakers against the First Amendment rights of listeners.").

4. GDPR, *supra* note 1, at 49–50.

5. *See* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 26 (1992) ("For virtually every commentator, however, the fundamental issue has been the loss of human dignity, autonomy, or respect that results from a loss of control over personal information.").

6. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 885 (1997) (calling the internet the "new marketplace of ideas"); Julie E. Cohen, *Information Privacy Litigation As Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 576 n.129 (2017) ("The information industries and their advocates in pro-business and libertarian think tanks have consistently argued that striking the proper balance between privacy and innovation is not a job for regulators . . . ."); Morgan N. Weiland, *Expanding the Periphery and Threatening the Core: The Ascendant Libertarian Speech Tradition*, 69 STAN. L. REV. 1389, 1399 (2017) ("[T]he libertarian tradition justifies and generates increasingly diverse and dissonant applications of the speech right that focus exclusively on corporate speech. For example, corporations have invoked the First Amendment as a defense against regulations ranging from statutes that prohibit the use of records about physicians' prescribing practices for marketing purposes and federal regulations prohibiting Internet service providers (ISPs) from discriminating against traffic from disfavored sources to statutes outlawing misleading statements by companies to investors."); Tim Wu, *The Right to Evade Regulation: How Corporations Hijacked the First Amendment*, NEW REPUBLIC (June 2, 2013), https://newrepublic.com/article/113294/how-corporations-hijacked-first-amendment-evade-regulation [https://perma.cc/PKR9-SQS8] ("Once the patron saint of protesters and the disenfranchised, the First Amendment has become the darling of economic libertarians and corporate lawyers who have recognized its power to immunize private enterprise from legal restraint."); Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1210 (2005)

The enforceable right to erasure obligates companies operating in Europe to limit commercial audiences' access to information that a natural person would want to keep out of the public eye. This Essay examines the GDPR's privacy policies and contrasts them from the U.S. preference for augmenting information available to audiences. It further critiques current U.S. recalcitrance in matters of commercial internet governance and suggests limited U.S. regulatory reform.

The 2018 regulation requires changes to the operations of U.S. internet intermediaries that operate within the European Union.[7] They will no longer be able to indefinitely retain users' data on their servers, nor will they be able to unlimitedly sell or resell them to third parties.[8] Several scholars have warned that the GDPR threatens free speech in the United States.[9] The territorial reach of the GDPR extends to businesses that run EU offices or "that collect, process or store the personal data of anyone located within an EU country."[10] In the first

---

(asserting that "the First Amendment critique can be located within the broader strand of First Amendment thought that believes, drawing upon libertarian theory, that the First Amendment guarantees not just freedom of speech for individuals, but also for business interests, and that many economic regulations conflict with the First Amendment").

7. Sheera Frenkel, *Tech Giants Brace for Europe's New Data Privacy Rules*, N.Y. TIMES (Jan. 28, 2018), https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html [https://perma.cc/Y2YS-5NMR]; Fouad Khalil, *Europe's Privacy Law Set To Change How Personal Data Is Handled Around the Globe*, THE HILL (Dec. 27, 2017), http://thehill.com/opinion/cybersecurity/366607-europes-privacy-law-set-to-change-how-personal-data-is-handled-around [https://perma.cc/E4ZA-6483].

8. Stefania Alessi, *Eternal Sunshine: The Right to Be Forgotten in the European Union After the 2016 General Data Protection Regulation*, 32 EMORY INT'L L. REV. 145, 155 (2017) ("The Internet's capacity to store information indefinitely was in tension with the text of the Directive, especially where the Directive provided that controllers could store personal data 'for no longer than is necessary for the purposes for which the data were collected or . . . processed.'" (quoting Data Protection Directive of 1995, Council Directive 95/46, 1995 O.J. (L 281) 31)).

9. *See, e.g.*, Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 984 (2018).

10. *What Countries are Affected by the GDPR?*, HIPAA J. (Apr. 17, 2018), https://www.hipaajournal.com/what-countries-are-affected-by-the-gdpr/ [https://perma.cc/34L9-XD3V] (concerning the GDPR's global effects); Joseph J. Lazzarotti et al., *Does the GDPR Apply to Your US-based Company?*, JACKSON LEWIS (Jan. 8, 2018), https://www.workplaceprivacyreport.com/2018/01/articles/international-2/does-the-gdpr-apply-to-your-us-based-company/ [https://perma.cc/6LYR-F3CB] ("The GDPR replaces the 1995 EU Data Protection Directive which generally did not regulate businesses based outside the EU. However, now even if

place, companies must provide clear terms to obtain users' consent for commercializing their private data and to subsequently enable them to withdraw that consent.[11] In addition, the GDPR prohibits internet intermediaries from obscuring how and for what purpose consumer data is collected. They must make transparent the procedures for erasure.[12] Data subjects must be given notice of breaches to internet intermediaries' systems likely to "result in a risk for the rights and freedoms of natural persons." Moreover, the data controller must hold only the minimum amount of data necessary to "protect the rights of data subjects."[13] The EU emphasis on safeguarding personal data contrasts from the U.S. Supreme Court's preference for the interests of commercial vendors and their audiences.

Members of the European Union, such as France and Germany, have developed domestic laws to meet the criteria set out in the GDPR.[14] The European Union's approach addresses the increasing power that social media companies wield by retaining and analyzing a treasure trove of personal data saved on corporate servers. Besides keeping information indefinitely, firms reap billions of dollars in profits by trading in data or selling access to it for marketing and political advertisement. The increasingly common capitalization of private facts is often done clandestinely, without the data subjects'

---

a US-based business has no employees or offices within the boundaries of the EU, the GDPR may still apply.").

11. GDPR, *supra* note 1, at 6 ("Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.").

12. *Id.* at 35 (requiring that personal data be "processed lawfully, fairly and in a transparent manner in relation to the data subject").

13. *GDPR Key Changes*, EU GDPR.ORG, https://www.eugdpr.org/the-regulation.html [https://perma.cc/MBZ3-LFHN]. Data subjects are defined as natural persons. GDPR, *supra* note 1, at 33 ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . . .").

14. THE LAW LIBRARY OF CONGRESS, LAWS ON ERASURE OF ONLINE INFORMATION 4–8 (2017).

knowledge.[15] Intimate and public information is obtained through transactions and internet searches.

There is widespread public ignorance about the extent to which data is sold and resold. Third-party vendors bury privacy statements in contracts of service with nebulous terms that demand full data-analytical control over personal data in exchange for social media or search engine services.[16] The terms of the privacy statements are typically so obscure and misleading that few even venture to read them.[17] For instance, Google misleadingly told users that by turning off the Location History function of their Android phones they would not be tracked, but failed to divulge that even then background apps continue to track their whereabouts.[18] Apple iPhones have a similarly misleading tracking function.[19] Moreover, a German

---

15. Grant Arnow, *Apple Watch-ing You: Why Wearable Technology Should Be Federally Regulated*, 49 LOY. L.A. L. REV. 607, 614 (2016) ("Much of . . . 'big data' is collected without consumer awareness and is sold for a variety of commercial purposes."); Meglena Kuneva, EU Consumer Commissioner, Address at Lisbon Council Event: A Blueprint for Consumer Policy in Europe: Making Markets Work with and for People (Nov. 5, 2009), http://europa.eu/rapid/press-release_SPEECH-09-515_en.htm [https://perma.cc/Z6B8-5L5W] (stating that "collection of personal and behaviour data" through technology "is currently being done on an unprecedented scale on a massive scale and mostly without any user awareness at all").

16. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 150 (2017) ("The FTC's assumed premise is that an imagined reasonable consumer read a privacy statement and agreed to the terms in it as well as other aspects of a consumer's impressions of the company's privacy representations. . . . The deceptive merchant, then, flouted this reasonable individual's consent. In reality, most consumers do not read privacy policies and are unaware of company's data policies."); *see also* Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 105 (2017); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 495 (2016).

17. My anecdotal experience is that even academics tend not to read internet privacy provisions. *See also* Mark Daniel Langer, *Rebuilding Bridges: Addressing the Problems of Historic Cell Site Location Information*, 29 BERKELEY TECH. L.J. 955, 970 n.118 (2014) (reporting that "when Google and Facebook updated their privacy policies in 2012, a survey found that the changes to the policies were too confusing for customers to understand"); Alison C. Storella, *It's Selfie-Evident: Spectrums of Alienability and Copyrighted Content on Social Media*, 94 B.U. L. REV. 2045, 2080 (2014) (stating, based on studies, that "many users simply do not know or understand how social media privacy settings work"); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 697 (2013) ("[E]vidence suggests that many users of Facebook do not understand how their privacy settings work in practice.").

18. *Google Records Your Location Even When You Tell It Not To*, GUARDIAN (Aug. 13, 2018), https://www.theguardian.com/technology/2018/aug/13/google-location-tracking-android-iphone-mobile [https://perma.cc/D7R8-NW3S].

19. *Id.*

judge found that "Facebook hides default settings that are not privacy-friendly in its privacy center and does not provide sufficient information about it when users register."[20] This judge's statement about Facebook's privacy policy can well be extended to other social media platforms. The European Union has determined that data subjects' privacy concerns sometimes outweigh commercial audiences' desires for greater volumes of commodified personal data.

In contrast to European law's preference for a natural person's privacy, U. S. law relies on an implied consent regime, assuming that users should simply diminish their privacy expectations for personal data once it has been tendered to commercial third parties. The idea is that audiences should be able to benefit commercially from accumulated private and public facts.[21] This notion is premised on the argument that social media companies need to retain a wealth of private information to better tailor search results.[22] And indeed, without being able to access the plethora of data available online, much of the purpose and power of speech would be lost. The freedom to speak implies the right to receive ideas and information.[23] The U.S. Supreme Court has recognized audiences' rights to access information in a variety of cases involving legal matters as diverse as public, journalistic access to trials[24] and the acquisition of dissident, political literature.[25] So too, in the campaign financing area, the Court has articulated audiences' right to obtain useful information for arriving at political decis-

---

20. *German Court Finds Facebook Guilty of Privacy Violations*, DEUTSCHE WELLE (Feb. 12, 2018), http://www.dw.com/en/german-court-finds-facebook-guilty-of-privacy-violations/a-42553867 [https://perma.cc/8LF9-3U77]; *Facebook Broke German Privacy Laws, Court Rules*, BBC NEWS (Feb. 12, 2018), http://www.bbc.com/news/technology-43035968 [https://perma.cc/DYL7-GK6C] (explaining that the German court found Facebook's pre-click policy to be insufficient for providing consumers notice).

21. Seagrumn Smith, *Microsoft and the European Union Face Off over Internet Privacy Concerns*, 1 DUKE L. & TECH. REV. 14, 1–4 (2002) (comparing the U.S. opt-out approach with the European opt-in approach). The Supreme Court first recognized the First Amendment right to gain useful information in *Lamont v. Postmaster General*, 381 U.S. 301 (1965).

22. ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU 33–34 (2011).

23. Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("[T]he Constitution protects the right to receive information and ideas.").

24. Gannett Co. v. DePasquale, 443 U.S. 368 (1979).

25. *Lamont*, 381 U.S. at 310.

ions.[26] Likewise, in the commercial realm, listener benefit is determinative in First Amendment jurisprudence.[27] U.S. precedents also allow lawmakers to balance national security concerns against the desires of interested audiences to travel abroad.[28]

However, the First Amendment's protection of audiences' access to "social, political, esthetic, moral and other ideas and experiences"[29] does not imply that commercial entities have any constitutional right to indefinitely retain and manipulate psychometric details about internet users. Profiting from and reselling data has a substantial effect on interstate economic activity and therefore places regulation of digital media companies within congressional Commerce Clause authority.[30] Contrary to EU policy, the United States has continued allowing for-profit internet information providers to gather an unlimited amount of information about data subjects.

The default for U.S. internet transactions is that if the data subject has not opted out of online tracking service, then that natural person's data can be resold to third parties.[31] On the other hand, the European GDPR requires the data subject to opt in; that is, to grant limited written consent before the internet intermediary can post the information on the World Wide Web.[32] The U.S. system of virtually unlimited resale of information to third parties leaves data subjects vulnerable. Without adequate consent, data subjects have no way of knowing how much of their data has been transacted to third

---

26. Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 473 (2010).

27. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562–64 (1980).

28. Zemel v. Rusk, 381 U.S. 1 (1965).

29. Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969).

30. *See* United States v. Morrison, 529 U.S. 598 (2000) (holding that congressional Commerce Clause authority extends only to economic activity with a substantial effect on interstate commerce). For contrasting articles dealing with the implications of *Morrison* on congressional Commerce Clause authority, see Douglas W. Kmiec, *Rediscovering a Principled Commerce Power*, 28 PEPP. L. REV. 547 (2001); Alberto B. Lopez, *Forty Yeas and Five Nays—The Nays Have It:* Morrison's *Blurred Political Accountability and the Defeat of the Civil Rights Provision of the Violence Against Women Act*, 69 GEO. WASH. L. REV. 251 (2001).

31. For an extensive analysis of contemporary U.S. internet law see, Ieuan Jolly, *Data Protection in the United States: Overview*, PRACTICAL LAW (July 1, 2016), http://us.practicallaw.com/6-502-0467 [https://perma.cc/QA5N-R786]. The reader should bear in mind that internet law is an evolving discipline, and that even a recent document should be sourced to know its currentness.

32. GDPR, *supra* note 1, at 37.

parties. Once a person reveals details about such things as personal location, shopping habits, sexuality, sex, education, travel plans, and an infinite number of similarly revealing data points, the subject becomes almost powerless to demand that social media companies purge all collected and tracked information.[33] Europe, on the other hand, has passed legislation to check corporate abuse of private data, reducing the risk that it will be transmitted to third parties against the will of the data subject.[34] The U.S. model is based on a more libertarian analytical construct, while the European model is more concerned with the autonomy and dignity of the subject.[35]

This essay analyzes the GDPR with an eye toward understanding how a similar provision could become U.S. law without violating the First Amendment. It compares and contrasts European policy preferences for privacy and dignity against virtually unlimited data collection in the United States. Europeans do not share the American romantic ideal of the commercial marketplace of ideas. This Essay further argues that U.S. courts should rely on an intermediate scrutiny standard to review regulations governing how long firms can commercially retain, market, and analyze identifiable information about

---

33. *Can You Really Delete Facebook Data?*, PBS NEWS HOUR (Apr. 15, 2018), https://www.pbs.org/newshour/show/can-you-really-delete-facebook-data [https://perma.cc/4HSS-SYGS]; Zack Whittaker, *Facebook Does Not Erase User-Deleted Content*, ZDNET (Apr. 28, 2010), https://www.zdnet.com/article/facebook-does-not-erase-user-deleted-content/ [https://perma.cc/85QL-CUAS]; Russell Brandom, *Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense*, VERGE (Apr. 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy [https://perma.cc/5CQ9-HKBF]; Aimee Picchi, *OK, You've Deleted Facebook, but Is Your Data Still Out There?*, MONEYWATCH (Mar. 23, 2018), https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/ [https://perma.cc/PP5B-7XZ4]. A Facebook account can, nevertheless, be deactivated from public view. Alex Hern, *How To Protect Your Facebook Privacy*, GUARDIAN (Mar. 19, 2018), https://www.theguardian.com/technology/2018/mar/19/how-to-protect-your-facebook-privacy-or-delete-yourself-completely [https://perma.cc/B87T-5FN7].

34. Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 431 (2013) ("In contrast to U.S. laws, European laws set high compliance obligations for companies requiring them to protect the privacy and security of consumers' sensitive data, including sensitive data that is stored in a public cloud.").

35. Ronald J. Krotoszynski, Jr., *The Polysemy of Privacy*, 88 IND. L.J. 881, 906 (2013) ("Just as the public/private distinction helps to inform the framing of privacy in the United States and in Europe, the concept of autonomy as privacy, rather than human dignity, seems to reflect important cultural differences between the United States and the wider world.").

natural persons. Part I explains the values of the GDPR's right to erasure (formally known as the right to be forgotten), and Part II addresses a number of counterarguments advanced by U.S. academics.

I. THE RIGHT TO ERASURE, PRIVACY, AND COMMERCIAL SPEECH

In the digital age, audiences not only receive information, they also participate in the marketplace of ideas by embedding hyperlinks, registering likes, and emailing hyperlinks to others. Advertisers are well aware of the value of predictive data, purchasing and relying on it to stage campaigns based on psychometric profiles gathered through algorithms that exploit speakers' and listeners' past digital ticks, preferences, purchases, and habits. Information technology firms like Google, Facebook, and Twitter rely on personal data collected from willing users, many of whom are unaware of how broadly their information is disseminated to third party intermediaries, such as DoubleClick. Owned by Google, DoubleClick gathers information for commercial purposes, which has a substantial effect on interstate commerce.[36] That's enormously helpful to consumers of everything from housewares, clothing, or appliances, to television shows (e.g., Netflix or Twitch), transportation (e.g., Uber), or meal services (e.g., Blue Apron or Postmates). An increasing line of products, collectively known as the internet of things, contains tracking devices.[37] These include, for

36. Joanna Geary, *DoubleClick (Google): What Is It and What Does It Do?*, GUARDIAN (Apr. 23, 2012), https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring [https://perma.cc/N9Z7-4LD4].

37. For discussions about how the internet of things affects privacy, see Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475, 482 (2017) (describing how the internet of things raises privacy concerns of corporate and governmental information gathering); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 117 (2014) (discussing how existing law is unprepared to deal with privacy concerns involving the internet of things in matters that include "discrimination, privacy, security, and consent"); Dalmacio V. Posadas, Jr., *The Internet of Things: The GDPR and the Blockchain May Be Incompatible*, 21 J. INTERNET L. 1, 25 (2018) (explaining how the GDPR will place obligations of privacy and consent on companies developing the internet of things); Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS. 14 (2016) ("The 'Internet of Things' is a loosely defined term referring to a future in which everyday objects have built-in

example, a thermometer that tracks temperatures and transmits them to advertisers that are not obligated to follow healthcare privacy rules found in HIPAA.[38] Without adequate regulations, behemoth internet intermediaries can store an almost infinite amount of data points on users, limited only by technological capabilities rather than social policies.

The GDPR provides greater privacy protection than U.S. law. Like the European Union, the United States demonstrates a preference for truthful information, prohibiting false and misleading marketing in the commercial speech realm.[39] But the European Union has more robust privacy protections.[40]

The European approach better reflects the realities of the internet as an interactive space where subjects voluntarily share information with targeted audiences but become subject to involuntary data collection by commercial actors. Therefore, the GDPR's injunction that a controller of data, upon request from a data subject to "rectif[y] . . . inaccurate personal data concerning him or her," protects consumers against misappropriation and dissemination of false or misleading personal metrics.[41] This provision's use of gendered pronouns clearly identifies that the proper party beneficiary of this law is a natural person. The most important development for data privacy in 2018 has been the GDPR's Article 17 mandate, known as the "Right to erasure ('right to be forgotten')." (The name has been formally changed to "the right to erasure," although the use of "the right to be forgotten" remains the most commonly used referent to the concept.)

The right to erasure empowers persons, providing that the data subject "shall have the right to obtain from the controller

---

sensors and network connectivity, allowing them to send and receive data on their own—i.e., without human-to-human or human-to-computer interaction.").

38. Sapna Maheshwari, *This Thermometer Tells Your Temperature, Then Tells Firms Where to Advertise*, N.Y. TIMES (Oct. 23, 2018), https://www.nytimes.com/2018/10/23/business/media/fever-advertisements-medicine-clorox.html [https://perma.cc/42EW-EQ68].

39. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980).

40. Private networks have proven inadequate in preventing data security breaches, which have been significant; for example in September 2018, over 50 million Facebook accounts were breached because of a flaw in the company's algorithm. Mike Isaac & Sheera Frenkel, *Facebook Network Breach Affects up to 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html [https://perma.cc/VGZ6-GF4G].

41. GDPR, *supra* note 1, at 43.

the erasure of personal data concerning him or her without undue delay."[42] Data must be erased if they are "no longer necessary in relation to the purposes for which they were collected or otherwise processed."[43] The data subject can choose when to withdraw consent from retention of the data.[44]

A similar consumer protection should be enacted in the United States to restrict the period of time that personalized commercial data can be maintained on corporate servers. The U.S. Supreme Court reviews commercial speech using intermediate scrutiny[45] rather than the more stringent strict scrutiny reserved for content-based regulations of expression.[46] Intermediate scrutiny empowers courts to balance government interests in consumer protections against information intermediaries' commercial schemes.[47] The First Amendment, as conservative and liberal Justices agree, first and foremost protects expressions of "philosophy, religion, history, the social sciences, [and] the arts"[48]—not commerce, and much less the unregulated manipulation of personal information. Additionally, constitutional principles protect the right to debate divergently, pluralistically, and heatedly.

The online marketing strategy of vendors like Google, Twitter, Facebook, and Snapchat is to gather information needed to create commodifiable data profiles. This commercialization is not principally about diversity, deliberation, nor even aesthetic communications. Some limitation on the retention of data, modeled partly on the GDPR, would allow for balanced adjudication of matters arising from conflicts between data subjects and digital audiences.

---

42. *Id.*

43. *Id.*

44. *Id.* at 44.

45. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 573 (1980) (establishing the intermediate scrutiny test for commercial speech).

46. Reed v. Town of Gilbert, 135 S. Ct. 2218, 2231–32 (2015).

47. David S. Han, *Middle-Value Speech*, 91 S. CAL. L. REV. 65, 114–15 (2017) ("As many have noted, the essence of all intermediate scrutiny tests like the *Central Hudson* test is balancing.").

48. In *Alvarez*, a majority of justices recognized that core First Amendment rights include "philosophy, religion, history, the social sciences, the arts." *See* United States v. Alvarez, 567 U.S. 709 (2012); *id.* at 731–32 (Breyer, J., concurring, joined by Justice Kagan); *id.* at 751 (Alito, J., dissenting, joined by Justices Scalia and Thomas).

The GDPR's requirements apply to commercial data. The EU law clearly recognizes the special values of "processing for journalistic purposes and the purposes of academic, artistic or literary expression."[49] The GDPR makes no attempt to erase history, but instead attempts to maintain commercial relations that do not indefinitely intrude on data subjects' privacy.[50] Context matters. Commercial data collection done to increase social media companies' revenue differs from pure speech (politics, philosophy, sciences, aesthetics, and the like) not involving a profit motive. However, personal information collected by data brokers must be erased after some predefined length of time.[51] The length and extent to which cyberspace changes our relationship with information cannot be underestimated; never before have companies had so much access to personal information.

The European Union's policy of restricting the length and duration of data storage reflects an explicit recognition that the interests of speakers and listeners must sometimes yield to the interests of natural data subjects. European law gives greater protection to the safeguards of privacy, "including dignity, reputation, and personal honor."[52] The United States also

---

49. GDPR, *supra* note 1, at Art. 85(1).

50. Viviane Reding, Vice President of the European Comm'n, EU Justice Comm'r, Speech at Innovation Conference Digital, Life, Design: The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 22, 2012), http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm [https://perma.cc/R9H9-YU4C] ("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. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media.").

51. *See* Ronan Daly Jermyn, *Retention of Employment Records*, LEXOLOGY (Mar. 21, 2017), https://www.lexology.com/library/detail.aspx?g=a3cd2df0-30b9-496f-a038-aa51b8074646 [https://perma.cc/9BZR-9WM4] (referring to personal and sensitive data retained by employers).

52. Krotoszynski, Jr., *supra* note 35, at 917. Germany presents an example of a democracy that recognizes that personal control of data is constitutive to self-determination and freedom. *See* Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. & POL'Y 91, 104 (2013) (quoting Bundesverfassungsgericht [BVerfGE] [Federal Constitutional Court] 1983, 65 BVerfGE 1 (41) (Ger.)).

recognizes the legal statuses of dignity and reputation, but in other contexts.[53]

When it comes to the First Amendment, however, U.S. perspective differs significantly. The United States is substantially more tolerant of the dissemination of personal information to third parties.[54] The Supreme Court has taken a libertarian tack, typically finding that the interest in expression outweighs that of privacy.[55] Yet, the commercial speech doctrine recognizes the lower value of information disseminated to audiences in order to stimulate sales, rather than ideas.[56] In cases where data brokering has a substantial aggregate effect on the national economy,[57] Congress can enact a statute that protects

---

53. Lawrence v. Texas, 539 U.S. 558, 567 (2003) (discussing "dignity" in the context of sexual autonomy); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 757 (1985) (acknowledging defamation to be an injury to reputation).

54. Bartnicki v. Vopper, 532 U.S. 519, 525 (2001) (upholding the third-party right to lawfully acquire meaningful information).

55. This short Essay does not allow me space to elaborate any further on the libertarian nature of U.S. free speech jurisprudence. In recent years, First Amendment jurisprudence has increasingly sided with corporate interests ahead of consumer protection laws. *See, e.g.*, Expressions Hair Design v. Schneiderman, 137 S. Ct. 1144 (2017); Sorrell v. IMS Health Inc., 564 U.S. 552 (2011). In previous works, I have discussed the libertarian trends in U.S. law. *See, e.g.*, Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 688 (2017); Alexander Tsesis, *Free Speech Constitutionalism*, 2015 U. ILL. L. REV. 1015, 1064; Alexander Tsesis, *Burning Crosses on Campus: University Hate Speech Codes*, 43 CONN. L. REV. 617, 620 (2010). For a recent effort to disentangle speech libertarianism from historically dated economic libertarianism, see Jane Bambauer, *First Amendment Watch Roundtable: Jane Bambauer Responds to Louis Michael Seidman*, FIRST AMENDMENT WATCH (June 28, 2018), https://firstamendmentwatch.org/first-amendment-watch-roundtable-jane-bambauer-responds-to-louis-michael-seidman/ [https://perma.cc/TM5Q-EAKX]. And for a refutation of Bambauer, see Michael Seidman, *First Amendment Watch Roundtable: Louis Michael Seidman Rejoinder*, FIRST AMENDMENT WATCH (June 28, 2018), https://firstamendmentwatch.org/first-amendment-watch-roundtable-louis-michael-seidman-rejoinder/ [https://perma.cc/2TXZ-XSUS]. Professor Fred Schauer provides a compendium of spurious lower court First Amendment challenges to reasonable regulations, including the Security and Exchange Commission's financial disclosure requirements; gambling laws; therapeutic counseling; franchise agreements; hygienic, professional rules; and labor announcements. Frederick Schauer, *The Politics and Incentives of First Amendment Coverage*, 56 WM. & MARY L. REV. 1613, 1614–16 (2015).

56. *See, e.g.*, Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) (affording "commercial speech a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values").

57. N. Am. Co. v. SEC, 327 U.S. 686, 705 (1946) ("[The] commerce clause does not operate so as to render the nation powerless to defend itself against economic forces that Congress decrees inimical or destructive of the national economy.").

consumers against social technology companies whose business models rely on the resale of psychometric data to third-party advertisers. Audiences' desire to acquire lucrative information should sometimes give way to claims of privacy. In *Cox Broadcasting Corp. v. Cohn*, the Court asserted, "[i]n this sphere of collision between claims of privacy and those of the free press, the interests on both sides are plainly rooted in the traditions and significant concerns of our society."[58] However, absent a statutory remedy, the U.S. Supreme Court favors the right of speakers to communicate information to audiences so long as it is lawfully acquired.[59] The key to resolving clashes between data-subject privacy and listener desire to acquire information is to create a statutory scheme adequately balancing the interests in digital environments. The GDPR provides just that model for developing comprehensive U.S. privacy protections.

Without adequate consumer protections, little is done to stop U.S.-based firms from amassing, reselling, analyzing, quantifying, and commodifying collected data. The Federal Trade Commission rarely enforces social media privacy agreements with users.[60] Additional U.S. law should explicitly recognize digital privacy as a right that in some cases, such as those involving reputational harms, counterbalances commercial audiences' desires to access information.[61]

The European Union has formalized a data subject's objective, human right to privacy,[62] even in the face of audiences who desire his or her personal information. The advantage of a

---

For a classic study on Commerce Clause and national economic matters, see Robert L. Stern, *The Commerce Clause and the National Economy, 1933-1946*, 59 HARV. L. REV. 645 (1946).

58. 420 U.S. 469, 491 (1975).

59. Florida Star v. B.J.F., 491 U.S. 524, 541 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979).

60. Samantha Cutler, Note, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1538 n.187 (2018) ("Internet privacy laws in the United States are enforced by the FTC, which can only go after businesses that violate their own privacy policies.").

61. *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985) (holding that "the false statements in the credit report did not involve matters of public concern which would require showing of actual malice for recovery of presumed and punitive damages").

62. European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, https://www.echr.coe.int/Documents/ConventionENG.pdf [https://perma.cc/EQY9-49T7].

public policy that favors privacy over indefinite data retention and distribution is evident from the manipulation of private data during the 2016 U.S. presidential election, when Facebook granted Cambridge Analytica ("CA"), a business specializing in manipulating digital profiling for targeted political advertisement, access to hundreds of thousands of user profiles and millions of associated friends' profiles. This example demonstrates the danger of a corporate entity, with no obligation to any constituency other than its investors, amassing and exploiting digital profiles. In all, CA obtained and then harvested at least 87 million Facebook profiles to improve marketing outcomes.[63] Facebook users were given no direct notice nor did they consent to this or comparable transactions, which stored and analyzed their personal and biometric information.[64] Absent civil rights or criminal remedies, "research has consistently shown that users of online platforms rarely adjust default privacy settings and often fail to understand what information they are sharing."[65] The fact that users could have used Facebook's architectural features to deny third parties access to personal information is therefore insufficient to protect private information. By relying on artificial intelligence to extract biometrics from the demographics gleaned from data subjects' profiles,[66] CA was not simply a passive listener. It orchestrated emotionally charged political campaigns that advanced demeaning, racialized, nationalistic propaganda,[67] which were primarily, albeit not exclusively, used by the Trump and other Republican political campaigns.[68]

---

63. Craig Timberg et al., *Facebook: 'Malicious Actors' Used Its Tools to Discover Identities and Collect Data on a Massive Global Scale*, WASH. POST (Apr. 4, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/ [https://perma.cc/G5DM-ZFQE].

64. A pending lawsuit alleges that Facebook sells biometric information in violation of state law. Ally Marotti, *Facebook Could Be Forced to Pay Billions of Dollars over Alleged Violations of Illinois Biometrics Law*, CHI. TRIB. (Apr. 17, 2018), http://www.chicagotribune.com/business/ct-biz-facebook-tagging-privacy-lawsuit-20180417-story.html [https://perma.cc/J7B4-D3HF].

65. Timberg, *supra* note 63, at § 7.

66. Tristan Greene, *Killer Robots? Cambridge Analytica and Facebook Show Us the Real Danger of AI*, NEXT WEB (Mar. 21, 2018), https://thenextweb.com/artificial-intelligence/2018/03/21/killer-robots-cambridge-analytica-and-facebook-show-us-the-real-danger-of-ai/ [https://perma.cc/WWQ3-LWXZ].

67. Vann R. Newkirk II, *White Supremacy Is the Achilles Heel of American Democracy: Even in a High-tech Era*, ATLANTIC (Apr. 17. 2018), https://www.theatlantic.com/politics/archive/2018/04/white-supremacy-is-still-americas-biggest-

Regulators and lawmakers never did step into this hideous breach of American normative and narrative principles about fair elections.[69] Nor under existing U.S. rules and standards were they required to take regulatory action.[70] An author's probing, rhetorical question reveals the dangers at stake: "[C]an you imagine what Hitler would have done with access to Facebook data on tens of millions of people?"[71] American social media companies provide tyrants with platforms for communications. Google is returning to the Chinese market, working with that country's government to censor searches as it had prior to 2010.[72] When the internet becomes instrumental to tyrannical governments—like the current ruling powers in Iran, China, Pakistan, Burma, Syria, and Saudi Arabia—these data readily lend themselves to repression, arrest, and torture.[73]

---

security-threat/557591/ [https://perma.cc/L5YE-H2XC]; Elyse Wanshel, *Cambridge Analytica Brags That It, Not Trump, Came Up with 'Crooked Hillary'*, HUFFINGTON POST (Mar. 21, 2018), https://www.huffingtonpost.com/entry/cambridge-analytica-crooked-hillary-nickname_us_5ab28131e4b054d118df06b3 [https://perma.cc/FF88-MASP].

68. Rhett Jones, *Authorities Seek Warrant to Raid Offices of Cambridge Analytica Amid Facebook Data Showdown*, GIZMODO (Mar. 18, 2018), https://gizmodo.com/authorities-seek-warrant-to-raid-offices-of-cambridge-a-1823901299 [https://perma.cc/6LY6-6FTF]; Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/YYW9-8U74]; Craig Timberg & Elizabeth Dwoskin, *A Voter Profiling Firm Hired by Trump Likely Grabbed Data for Tens of Millions of Facebook Users*, WASH. POST (Mar. 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/17/a-voter-profiling-firm-hired-by-trump-likely-grabbed-data-for-tens-of-millions-of-facebook-users/? [https://perma.cc/P4NR-FV6W].

69. On the interwoven relation between legal institutions, norms, narratives, and interpretation, see Robert M. Cover, *Nomos and Narrative*, 97 HARV. L. REV. 4 (1983).

70. Alistair Smout, *UK Lawmakers Publish Evidence from Cambridge Analytica Whistleblower*, REUTERS (Mar. 29, 2018), https://www.reuters.com/article/us-facebook-cambridge-analytica-britain/uk-lawmakers-publish-evidence-from-cambridge-analytica-whistleblower-idUSKBN1H51VW [https://perma.cc/UUZ3-2HVD].

71. Justin Bariso, *Facebook, Cambridge Analytica, and the Dark Side of Emotional Intelligence*, INC. (Mar. 26, 2018), https://www.inc.com/justin-bariso/facebook-cambridge-analytica-dark-side-emotional-intelligence.html [https://perma.cc/9KCP-QRQT].

72. *The World This Week*, ECONOMIST, Aug. 4, 2018, at 5.

73. Sharon Kelly McBride, *Tell President Obama to Put Human Rights First in His Inaugural Address*, HUM. RTS. FIRST (Jan. 17, 2013), http:// www.humanrightsfirst.org/2013/01/17/tell-president-obama-to-put-human-rights-first/ [https://perma.cc/GGF6-A2CF] (listing some countries that suppress dissent on social media). For individual details about how specific autocracies abuse their citizens' privacy, see Sreeram Chaulia, *A Pressing Matter*, FIN. EXPRESS, May 7, 2010, at 9,

While the United States and European Union are pluralistic in their approaches to communication, external forces seek to undermine their democracies. In fact, U.S. intelligence services—specifically the FBI, CIA, and NSA—found that Russian intelligence services hacked a Democratic Party email server. Wikileaks later disseminated documents that it very likely obtained from the Russian government, becoming, in the view of the FBI and CIA directors, either an advertent or inadvertent agent of the Russian Intelligence Services.[74] EU law limits access to users' social media accounts and other sources of private information in order to prevent governments and private corporations from amassing and analyzing information without obtaining data subjects' actual consent.

"Consent" should not be an ambiguous term, neither in EU nor U.S. regulations. The European Union's directive provides a clear definition of the term. The GDPR requires an internet intermediary to receive "unambiguous" consent to retain a subject matter's data in its servers.[75] Regulators will need to periodically check whether a social media company's business practices follow this directive.

---

http://www.sreeramchaulia.net/publications/PressPredators.htm [https://perma.cc/YTQ7-M2B8] (Saudi Arabia); Peter Goodspeed, *Goodspeed Analysis: The Arab Spring May Have Helped Usher in a New Era of Government Surveillance*, NAT'L POST (Apr. 21, 2012, 1:08 AM), https://nationalpost.com/opinion/goodspeed-analysis-governments-could-soon-record-and-store-everything-their-citizens-do-from-birth-to-death [https://perma.cc/ZQB2-4SA8] (Iran); *UN Paints Bleak Rights Picture in Iran*, RADIO FREE EUR. RADIO LIBERTY (Oct. 12, 2012), http://www.rferl.org/content/iran-human-rights-united-nations-/24736902.html [https://perma.cc/ZX4U-UKHD] (same); John Gregory, *Government Control of the Internet*, SLAW (Jan. 16, 2013), http://www.slaw.ca/2013/01/16/government-control-of-the-internet/ [https://perma.cc/8GWX-7GWQ] (Syria); John Markoff & David Barboza, *Hackers from China Hit Gmail, Google Says*, N.Y. TIMES, June 2, 2011, at B1 (China); *Internet in Pakistan Is "Not Free": Report*, EXPRESS TRIB. (Sept. 25, 2012), http://tribune.com.pk/story/441949/internet-in-pakistan-is-not-free-report/ [https://perma.cc/GL2C-RNQM] (Pakistan); Aung San Suu Kyi, *"Too Busy to Tweet"*, YAHOO NEWS PHIL. (Sept. 18, 2011), http://ph.news.yahoo.com/aung-san-suu-kyi-too-busy-tweet-045259614.html [https://perma.cc/64QA-3EJQ] (Burma).

74. Ellen Nakashima et al., *Hacker Offers Glimpse of Assange's Secret World*, WASH. POST, Jan. 18, 2018, at A1 ("The three major U.S. intelligence agencies—the CIA, the FBI and the National Security Agency—assessed 'with high confidence' that Russia relayed to WikiLeaks material it had hacked from the Democratic National Committee and senior Democratic officials."); Kathryn Watson, *How Did WikiLeaks Become Associated with Russia?*, CBS NEWS (Nov. 15, 2017, 1:11 AM), https://www.cbsnews.com/news/how-did-wikileaks-become-associated-with-russia/ [https://perma.cc/3MU6-775M].

75. GDPR, *supra* note 1, at 34.

A specified length of time should be established for the storage and maintenance of business records. That duration should be set to protect consumers, who often do not know how to alter and set privacy settings in platforms like Facebook and Twitter. Any material the data subject inadvertently shares can be resold to an untold number of third-party e-companies and governmental entities. In the United States, where the same stringent data protections do not apply as in Europe, data marketers can indefinitely turn psychometric evaluations into profits.

Algorithmic evaluations crunch tens of thousands of uniquely identifiable data points that can only grow with the expansion of the internet. To combat the privacy threats, the EU has determined that consumers have a regulatory right to demand that data platforms limit their analyses; put another way, a private data subject should not be forced to reveal him- or herself to commercial audiences indefinitely and against his or her personal consent. Without regulations there is nothing keeping corporations, which by definition have perpetual life, from indefinitely data mining stale information. Companies like Acxiom, Experian, and Infogroup seek to augment, not shed, the slew of information far beyond anything that had ever been fathomable in human history.[76]

Viviane Reding, when she was European Commissioner for Education and Culture, proposed advancing privacy protections to safeguard human safety and dignity. Reding regarded data protection to be "the currency of today's digital market." Like any other commodity, she believed EU data protection should provide "stability and trust," encouraging creativity while "protecting people's fundamental right to data protection."[77] The GDPR should go further. It should, for example, prohibit companies doing business in Europe from transferring data to the United States. That the law lacks such a provision enables U.S. social media companies operating in Europe to minimize the

---

76. *See* Natasha Lomas, *Cambridge Analytica's Nix Said It Licensed 'Millions of Data Points' from Acxiom, Experian, Infogroup to Target US Voters*, TECHCRUNCH (June 6, 2018), https://techcrunch.com/2018/06/06/cambridge-analyticas-nix-said-it-licensed-millions-of-data-points-from-axciom-experian-infogroup-to-target-us-voters/ [https://perma.cc/7K5Q-UU48]; Tom Bergin, *How a Data Mining Giant Got Me Wrong*, REUTERS (Mar. 29, 2018), https://www.reuters.com/article/us-data-privacy-acxiom-insight/how-a-data-mining-giant-got-me-wrong-idUSKBN1H513K [https://perma.cc/4GA5-8NWS].

77. Reding, *supra* note 50, at 2, 3.

GDPR's effectiveness. In April 2018, *The Guardian* newspaper reported that Facebook was transferring 1.5 billion users' data from Ireland to California in order to avoid complying with EU's transparency and erasure laws.[78]

A 2012 study of EU citizens found that their data typically includes personal information disclosed through social networking sites or online shopping. Seventy-two percent of respondents were concerned about giving away their personal data for unrelated company uses, 75 percent wanted to be able to delete personal information that they had previously transmitted online, and 90 percent of Europeans interviewed were "in favour of equal data protection rights across Europe."[79] The GDPR empowers people to decide whether and the extent to which they are willing to allow companies to maintain data when they are no longer being operationalized for the purpose a data subject volunteered to have it processed.[80] In the United States, to the contrary, social media intermediaries have even monetized the content of emails.[81] The GDPR's right to erasure restricts firms from indefinitely retaining and processing stale and irrelevant data. The outer limits of data retention should be determined by policy considerations rather than the outermost limits of technological advancements.[82]

The GDPR is a consumer protection law:

---

78. Alex Hern, *Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law*, GUARDIAN (Apr. 19, 2018), https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law [https://perma.cc/D9J3-VJKV].

79. European Commission, Europe this Week (Jan. 27, 2012), http://europa.eu/rapid/press-release_ETW-12-2701_en.pdf [https://perma.cc/BJT3-SEZ7].

80. European Commission Memorandum MEMO/13/923, LIBE Committee Vote to Back New EU Data Protection Rules 1, Oct. 22, 2013 (europa.eu/rapid/press-release_MEMO-13-923_en.doc? [https://perma.cc/E33A-HGJD]).

81. Douglass MacMillan, *Tech's 'Dirty Secret': the App Developers Sifting Through Your Gmail*, WALL ST. J. (July 2, 2018 11:14 AM), https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442 [https://perma.cc/3GV7-9PXN]; Viviane Reding, Vice President of the European Comm'n, Justice Commissioner, Speech at Intervention in the Justice Council 5 (Mar. 8, 2013), http://europa.eu/rapid/press-release_SPEECH-13-209_en.pdf [https://perma.cc/7CBK-L3BW] ("Risks to privacy remain and are real. A single piece of data such as an email address can create a link between a very accurate profile and a person. It is particularly important to keep this in mind since pseudonymous data is often used in the health sector.").

82. Reding, *supra* note 50.

> [A] data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation.[83]

The GDPR additionally empowers anyone who consented as "a child and . . . not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet."[84]

Because the GDPR just became law in 2018, uncertainty remains about how the right to erasure will be implemented. Data-mining corporations, like Facebook, Google, or Bing, will need to be proactive, but their profit interests are counter-regulatory.[85] Nevertheless, periodic government audits should help identify whether these firms are properly notifying clients about what they share with third parties and of the identity of those transactional entities.[86] The data subject should also have access to his or her information within a reasonable time after making a formal request to a data firm in order to remain aware and verify that personal information is not being unlawfully stored in data intermediaries' servers.[87] These are not perfect solutions but good starts to significantly fortify consumer privacy laws. The right to erasure is not absolute. European states must reconcile data subjects' interests in pri-

---

83. GDPR, *supra* note 1, at 12.

84. *Id.* at 13.

85. Regulatory safeguards are needed to deter data companies from underspending on data security, sometimes resulting in loss of personal and public data to third parties. *See, e.g.*, John D. Sutter, *Google Maps "Loses" Major Florida City*, CNN (Sept. 22, 2010, 5:31 PM), http://www.cnn.com/2010/TECH/web/09/22/google.lost.sunrise.florida/index.html [https://perma.cc/X732-A2MP]; Victoria Woollaston, *Has Gmail Lost YOUR Emails? Glitch Causes Thousands of Users to Accidentally Delete Messages and Report Others as Spam*, DAILYMAIL (Jan. 29, 2014, 8:08 AM), http://www.dailymail.co.uk/sciencetech/article-2548010/Has-Gmail-lost-YOUR-emails-Glitch-causes-thousands-users-accidentally-delete-messages-report-spam.html [https://perma.cc/ECQ2-K2W2].

86. GDPR, *supra* note 1, at 12.

87. *Id.*

vacy with audiences' interests in journalism, artistic pieces, academic works, and literary expressions.[88]

The United States has passed no similarly comprehensive privacy regulation. Even neutral privacy protections would need to survive First Amendment analysis. Even content neutral regulations on the duration for which information intermediaries can retain data would need to meet a heightened level of scrutiny and be narrowly tailored to legitimate ends such as service efficiency and public safety.[89] If Congress were to adopt a statute with an opt-in provision similar to the European model, the federal commercial regulation would need to advance a substantial governmental interest.[90] A statute balancing the interests of privacy against a listener's right to know should protect dignitary interests, advance the marketplace of ideas, and provide consumers with the positive right to access their information. Audiences would continue to find an infinite amount of information while corporations would nevertheless be required to purge personally identifiable, yet stale data retained on the parent company's or subsidiaries' servers.

By retaining control over data, the data subject is empowered to prevent commercial vendors from sharing private, stale, and erroneous information that is likely to compromise personal dignity. Control over information, as legal scholar Julie Cohen has asserted, promotes autonomy and enhances human creativity.[91] In some instances, an audience's ability to access commercially maintained personalized files can adversely affect data subjects' self-definition, life trajectory, thoughts, ideas, and careers.

The marketplace of commerce is not the same thing as the marketplace of ideas. Commercial interests with a substantial effect on the national economy can be regulated to a greater

88. *Id.* at 28.

89. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011) (holding that a statute restricting "the sale, disclosure, and use" of pharmaceutical business records is subject to heightened judicial scrutiny).

90. *Id.* at 571–72 (stating that nondisclosure statutes targeting the dissemination of commercial data could only be sustained if the state could "show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest").

91. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1427 (2000) (stating that "[a] regime built on pervasive practices of monitoring, prediction, and preference-shaping is far more likely to stifle these habits of independent thought than to stimulate them").

extent than those that are aspects of personal autonomy in matters like politics, sociology, and philosophy. The same is of course true about the abstract topic of advertisement, which the First Amendment fully protects. For-profit forms of expression, however, are within congressional Commerce Clause authority.

Of course, the ability to obtain information is of value to curious audiences, but so too is the subjects' ability to maintain reasonable control over personal data. This is especially true when people seek to make heterodox, embarrassing, or politically risky statements online without being haunted by the prospect that companies like Cambridge Analytica will later commodify or politicize their psychometric profiles. The monetary exploitation of data by internet companies has a substantial effect on the national economy and is therefore within the purview of congressional Commerce Clause authority.[92]

National policy and collective action are needed to combat social media privacy intrusions.[93] As things currently stand, U.S. privacy protections are too piecemeal and inadequately suited for the digital environment. As Professor James Whitman, who writes about comparative aspects of privacy law, explains, the European Union's privacy protections, "are, at their core, a form of protection of a right to respect and personal dignity."[94]

---

92. Paul R. La Monica, *Tech's Top Five Now Worth More than $3 Trillion*, CNN (Oct. 31, 2017, 12:28 PM), http://money.cnn.com/2017/10/31/investing/apple-google-alphabet-microsoft-amazon-facebook-tech/index.html [https://perma.cc/Q7JK-4ZP9]; *see also* Felix Richter, *Google's Steady Climb Towards $1 Trillion*, STATISTA (Sept. 4, 2018), https://www.statista.com/chart/15326/google—alphabet-market-capitalization/ [https://perma.cc/KX53-WAVD]; Rani Molla, *Google's and Facebook's share of the U.S. ad market could decline for the first time, thanks to Amazon and Snapchat*, RECODE (Mar. 19, 2018), https://www.recode.net/2018/3/19/17139184/google-facebooks-share-digital-advertising-ad-market-could-decline-amazon-snapchat [https://perma.cc/WYC5-VTXH].

93. Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519, 595 (2012) (Ginsburg, J., dissenting in part) ("Congress' intervention was needed to overcome this collective-action impasse."); *see also* Neil S. Siegel, *Collective Action Federalism and Its Discontents*, 91 TEX. L. REV. 1937 (2013) (providing in-depth discussion of Justice Ginsburg's "collective-action impasse" comment).

94. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004). For discussions of German and French privacy protections, see Gerrit 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, 84–85 (2009) (discussing German privacy protections); Elisabeth Logeais & Jean-Baptiste Schroeder, *The*

Listeners' interests do not categorically supersede those of the data subjects. The dignity of maintaining some control over one's internet data enhances consumer protection against exploitation. Neither audience rights nor personal rights are absolute. In an online world, where phones with cameras and recording devices are virtually ubiquitous, conflicts arise between audiences' desires for greater access to private information shared on social media platforms and private persons' interests in maintaining control over their data.[95] Commercial actors have a special interest in acquiring accurate profiles of data subjects. Regulatory limits can be placed on information distribution. Even the Postal Service can refuse to deliver "pandering advertisements" upon an addressee's request.[96] U.S. policy makers must fashion law consistent with the Supreme Court's intermediate scrutiny precedents for reviewing commercial speech regulations. The GDPR places obligations on U.S. data firms and will perhaps influence legislative initiatives in Congress.[97]

The European Union recognizes that the prevention of long-term, and perhaps even permanent, reputational harms requires lawmakers to protect consumers against exploitative marketing. Advertising and data-collection laws expand consumers' choices and ability to make self-determined product and transactional assessments. The GDPR empowers data subjects to demand that firms remove their information when

---

French Right to Image: An Ambiguous Concept Protecting the Human Persona, 18 LOY. L.A. ENT. L.J. 511, 513 (1998) (discussing French privacy protections).

95. For an elaborate discussion about online conflicts between free speech and privacy, see DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007); Jacqueline D. Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919, 949 (2010) (developing an analytical model to preserve free speech and establish social norms for regulating digital video privacy). For a discussion about online conflicts between free speech and the right to be left alone, see Deana Pollard Sacks, Snyder v. Phelps, *the Supreme Court's Speech-Tort Jurisprudence, and Normative Considerations*, 120 YALE L.J. ONLINE 193, 193 (2010).

96. Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 729–30, 740 (1970); *see also* FCC v. Pacifica Found., 438 U.S. 726, 731 n.2 (1978).

97. Luci Handley, *US Companies Are Not Exempt from Europe's New Data Privacy Rules*, CNBC (Apr. 25, 2018, 5:43 AM), https://www.cnbc.com/2018/04/25/gdpr-data-privacy-rules-in-europe-and-how-they-apply-to-us-companies.html [https://perma.cc/Q6LD-BAKX]; Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business*, FORBES (Dec. 4, 2017, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/ [https://perma.cc/6R5F-EJTC].

it is no longer needed for the original transaction. Current U.S. law, to the contrary, does not require internet information providers to get prior consent from subjects and allows them to retain or transact in stale data.

On a national level, EU countries likewise protect the privacy of speakers against the commercial interests of audiences. The German concept of personal control, for instance, is closely related to the terms of the GDPR because it identifies personal control over one's data to be critical for self-determination and personal freedom. The German Constitutional Court has spoken to the importance of protecting private information in the digital age, asserting that dignity and human worth are "[a]t the heart of constitutional order."[98] Some regulations on the dissemination of private data are necessary to advance the ordinary functions of any democracy, including the United States. The right to privacy, Professor Jed Rubenfeld has pointed out, is a key component of democratic governance and serves as a barrier against totalitarianism.[99] U.S. lawmakers should learn from the EU's approach with the newly enforced GDPR.

While people enjoy a Fourth Amendment right of autonomy against law enforcement agencies' unreasonable searches, there currently is no U.S. law preventing data brokers who sell information to third parties from also dealing with police agencies.[100] Until the Supreme Court put an end to the practice

---

98. Larson, *supra* note 52, at 104 (quoting a decision by the German Federal Constitutional Court).

99. Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 802–05 (1989).

100. Amitai Etzioni, *Reining in Private Agents*, 101 MINN. L. REV. HEADNOTES 279, 285–88 (2016) (discussing the lack of legal limitations on disclosure of personal information by data brokers); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 843 (2016) ("The third-party doctrine resolves the Fourth Amendment question whether police can access the same personal information directly from the third-party provider. The answer is generally yes. If individuals give up personal information to third parties in return for better insights about health, fitness, or the like, then the third-party doctrine does not protect that information from police requests. Obviously, the choice is up to the third party whether to comply with police investigations without a warrant." (citations omitted)); Benjamin J. Priester, *Five Answers and Three Questions After* United States v. Jones *(2012), the Fourth Amendment "GPS Case"*, 65 OKLA. L. REV. 491, 522 (2013) ("Under the 'third-party doctrine' line of cases, no *Katz* reasonable expectation of privacy exists for this information, and therefore no Fourth Amendment 'search' occurs when the police obtain the information from the other party to the information exchange.").

in 2018,[101] private firms would almost indiscriminately sell information to law enforcement agents with no more than a subpoena, rendering the system an end run around the Fourth Amendment Search and Seizure Clause.[102] Amazon, for instance, sells face recognition technology to an untold number of law enforcement agencies.[103] More familiar is the commercial reselling of supposedly anonymized data that was the subject of litigation in *Sorrell v. IMS Health, Inc.*, where the Court struck down on First Amendment grounds a statute that had prohibited data mining in pharmaceutical prescription files.[104] In that case, the majority did not take into account that even the sale of anonymized personal information is not safe from resale to third-party vendors who can then deanonymize it.[105]

Peoples' rights against such intrusive audiences should be formally preserved to advance the interests of privacy and human dignity against private entities that engage in clandestine mining of data to reap billions of dollars in profits. The Supreme Court has recognized that the right to privacy against

---

101. Carpenter v. United States, 138 S. Ct. 2206, 2217, 2219 (2018) (holding that the Fourth Amendment requires a state to get a search warrant before gaining access to seven days' worth of cellphone site data that law enforcement agents had used for a criminal investigation).

102. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 330 (2008) ("Since virtually all information obtained through data mining comes from third party record holders—either the government itself, commercial data brokers, or a commercial entity like a bank—its acquisition does not implicate the Fourth Amendment."). The Fourth Amendment requires government to demonstrate probable cause through a preponderance of the evidence; whereas a court can issue a subpoena with a lower standard, upon reasonable grounds to believe that the evidence sought is relevant to a criminal investigation. Griffin v. Wisconsin, 483 U.S. 868 (1987).

103. Elizabeth Dwoskin, *Amazon Is Selling Facial Recognition to Law Enforcement*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/ [https://perma.cc/866Z-XR2B].

104. 564 U.S. 552, 579–80 (2011).

105. *See* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 446 (2018) (discussing the deanonymization of data that had initially been anonymized); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703 (2010) ("Clever adversaries can often reidentify or deanonymize the people hidden in an anonymized database."); Erica M. Scott, Comment, *Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is A Trans-Atlantic Browser-Based Opt-in for Behavioral Tracking the Right Solution?*, 26 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 285, 293 (2013) (discussing deanonymization methods).

abusive state actions exists in the penumbras of constitutional meaning.[106] In the same way, the right of association, guaranteed under the First Amendment contains a privacy component.[107] In other areas of law, too, the Supreme Court has recognized that self-determination is critical to intimate decisions, including abortions and sexual freedoms.[108] Likewise, marriage equality includes elements of maintaining human dignity against government interference. Therefore, a federal statute that interfered with equal dignity of same-sex couples to marry violated their fundamental right to privacy.[109] Furthermore, even inmates in prison have a right commensurate with "the essence of human dignity inherent in all persons."[110]

The Court's dignity jurisprudence should be brought up-to-date to preserve privacy against commercial audience overreach. Social media postings and those on other commercial internet intermediaries benefit consumers and businesses alike. Congress should, nevertheless, pass legislation empowering customers to remove personally identifiable data used by internet intermediaries for psychometrics, biometrics, and purposes otherwise unconnected to the original commercial transaction through which the social media company acquired the data. Courts should review those consumer protection laws under intermediate scrutiny, as they do with other commercial regulations.

---

106. Griswold v. Connecticut, 381 U.S. 479, 484 (1965). More recent cases, such as *Roe v. Wade*, ground privacy in Fourteenth Amendment doctrine. 410 U.S. 113, 153 (1973). But the Court has never outright overturned Justice Douglas's penumbral analysis in *Griswold*. To elaborate on this point any further would be beyond the scope of this Essay.

107. *Griswold*, 381 U.S. at 483 ("In *NAACP v. State of Alabama*, 357 U.S. 449, 462 [1958], we protected the 'freedom to associate and privacy in one's associations,' noting that freedom of association was a peripheral First Amendment right."); Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 569 (1963) ("The right of association has become a part of the bundle of rights protected by the First Amendment (see, e.g., N.A.A.C.P. v. Alabama [ ]), and the need for a pervasive right of privacy against government intrusion has been recognized, though not always given the recognition it deserves.").

108. Justice O'Connor has made clear that "marriage, procreation, contraception, family relationships, child rearing, and education" involve "choices central to personal dignity and autonomy." Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992).

109. United States v. Windsor, 570 U.S. 744, 770 (2013). In a separate case, finding unconstitutional a state statute that prohibited intimate homosexual contact, the Court explained that such a law negatively impacts the affected persons' dignities. Lawrence v. Texas, 539 U.S. 558, 575 (2003).

110. Brown v. Plata, 563 U.S. 493, 510 (2011).

Current U.S. law permits the unregulated resale of private data to third parties unrelated to the transaction that the consumer has entered.[111] Thereby, U.S. law sets inadequate limits on internet platforms—Google, Facebook, or similar commercial media—to remove posted statements, pictures, and other interactivity through their servers. Information technology companies algorithmically and synthetically translate information posted on their networks. Psychometric data are then used to sell products or to resell private information to third parties without sufficiently clear prior consent of data subjects. A limited right to erasure, modeled on the GDPR, leaves personal decisions in the hands of consumers rather than impersonal corporations.

Courts reviewing limits on the duration for which commercial entities can retain data subjects' information should rely on intermediate scrutiny.[112] That level of review is appropriate because such matters concern commercial speech, which is treated differently than core First Amendment expressions (such as philosophy, politics, aesthetics, and the like).[113] When a firm obtains private data through one transaction and then profits by commodifying it, the Federal Trade Commission should enforce its own Fair Information Practice Principles. Those guidelines require data collectors to provide consumers with "clear and conspicuous notice of their information practices, including what information they collect [and] how they collect it."[114]

---

111. *See* NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS, THINK BEFORE YOU DIG: PRIVACY IMPLICATIONS OF DATA MINING & AGGREGATION 3 (Sept. 2004), https://www.nascio.org/Portals/0/Publications/Documents/2004/NASCIO-dataMining.pdf [https://perma.cc/DA3U-3KKL] (noting that data may be used for multiple applications).

112. Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1274 (2007) ("Most challenged legislation will be upheld as long as it is even rationally related to a legitimate governmental interest; intermediate scrutiny demands a 'substantial' relationship between ends and means. As with the compelling interest requirement, strict scrutiny's demand for narrow tailoring or necessity is the most stringent made by any doctrinal test of constitutional validity.").

113. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563–64 (1980); *see* Fallon, *supra* note 112 and accompanying text.

114. FED. TRADE COMM'N, REPORT TO CONGRESS, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 36–37 (2000), http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/654M-X5YU]; FED. TRADE COMM'N, *Fair Information Practice*

If the United States were to adopt a measure comparable to the right to erasure, it should prohibit indefinite commercial retention of data, but it should not limit private retention of data, to which strict scrutiny would apply, as the latter would not trigger the commercial speech doctrine.[115] The GDPR recognizes the distinction between business and private storage. Article 2 of the EU regulation specifically "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[116] The GDPR further makes clear that the right to erasure does not include data gathered "by a natural person in the course of a purely personal or household activity."[117] Judicial oversight is not enough, however, because of the typical Article III limitations of standing, mootness, and ripeness. The intrusion into consumer privacy effected by the amassing and indefinite retention of private information requires appropriate statutory measures to regulate those internet intermediaries that have a substantial effect on interstate commerce.

II. FORESEEABLE COUNTERARGUMENTS

Several U.S. scholars have strongly opposed what most continue to refer to as, "the right to be forgotten." Professor Robert Post, for instance, expresses disfavor for delisting information available on search engines, such as Google. A limit on data retention, he believes, will be detrimental to the deliberative public sphere, which is essential to democratic self-

---

Principles, https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007) [https://perma.cc/4DY7-XF2K] (the "five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress").

115. There is a recent trend in the Supreme Court that may eventually alter this dichotomy. Much depends on whether Justices will continue moving to a more libertarian position. In dicta to the most recent case on data protection, *Sorrell v. IMS Health, Inc.*, the Court hinted that it might eventually apply the strict scrutiny test even to commercial data, but the majority found that only intermediate scrutiny was needed for it to hold the state law to be unconstitutional. 564 U.S. 552, 570–78 (2011). Therefore, the intermediate scrutiny test of *Central Hudson* remains good law. 447 U.S. at 566.

116. GDPR, *supra* note 1, at 32.

117. *Id.* at 3.

government.[118] His concerns should be taken seriously because public information is so essential to audience participation in democracy and for listeners' pursuit of self-expression; indeed, as we noticed before, the GDPR distinguishes between commercial data appropriation and public reporting or historic recording.[119] Post advocates for "close judicial supervision" to safeguard the legal system's concern for "free formation of public opinion" in order to stave "the curtailment of public discourse to achieve social goods."[120] A judicial balancing of privacy and commercial speech concerns would be welcome for the prevention of government overreaching and chilling of speech.

Other scholars have also opposed having a set limit on social media data retention. Professor Jane Yakowitz Bambauer is concerned that Article 17 of the GDPR will require internet intermediaries to remove humiliating and disreputable images. She regards removal of videos recorded in public to impose "serious costs on the public" because it erases a source of factual information.[121] But much of the data appearing online is not merely factual; rather, humiliating posts, revenge videos, and defamatory content regularly appear on the internet. Several authors have also pointed out the manipulative nature of many internet advertisements, which have social costs associated with interstate commerce.[122]

---

118. Post, *supra* note 9, at 1070. Post grounds his theory of free speech on the value of deliberation to democratic self-government. *See* Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, 88 CALIF. L. REV. 2353, 2362 (2000); Robert C. Post, *Between Democracy and Community: The Legal Constitution of Social Form*, *in* DEMOCRATIC COMMUNITY 163 (John W. Chapman & Ian Shapiro eds., 1993).

119. *See supra* note 50 and accompanying text.

120. Post, *supra* note 9, at 1071.

121. Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 260–61 (2012).

122. *See, e.g.*, Micah L. Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497, 522 (2015) (discussing how some online marketing seeks not to inform but to manipulate consumers by taking "advantage of consumers' cognitive weaknesses and biases"); George N. Root III, *Examples of Manipulative Advertising*, HOUSTON CHRON. (last updated Nov. 28, 2018), http://smallbusiness.chron.com/examples-manipulative-advertising-11668.html [https://perma.cc/Q6CM-UJQS]; Ramsi A. Woodcock, *The Obsolescence of Advertising in the Information Age*, 127 YALE L.J. 2270, 2275–76 (2018) ("Advertising in its manipulative guise, so far from smoothing the flow of commerce, threatens technological advance, by giving consumers a reason—image—to purchase a product that is distinct from the only reason for which a

Bambauer's point is predicated on the notion that the public audience has a legally cognizable interest in private data posted for whatever reasons on the internet. To the contrary, permanent data storage of digital behaviors—such as Google search histories, Facebook profiles, or similar commercial communications—is not, as Bambauer would have it, "public domain information . . . pertinent to the evaluation of a person."[123] Much of what we do online, including speaking about toiletries, where we live, where we shop, and whatnot, targets specific listeners but not the public at large. Consumer protection legislation, like the GDPR, requires companies to obtain specific consent before monetizing this information. A consent provision should be included in any U.S. analogue of that law.

Bambauer well understands that there are potential harms that arise from unlimited trading in personal digital data.[124] She concedes, therefore, that some amount of purging of data storage records is advisable. And, I may add, this should be done within a reasonable period of time. Indeed, some data that is spread online is by no means benign. Ethnically, religiously, and racially charged rumors disseminated on Facebook have instigated violence in countries from Sri Lanka to Indonesia, Israel, India, and Mexico.[125] The problem becomes increasingly acute as Facebook displaces local media with news stories impugning the reputations of identifiable groups like Muslims, Jews, and LGBT people going viral on social media and being taken up by violent organizations seeking to harm the specters of their animus.

Social interests in reputation and the marketplace of ideas sometimes trump the interests of audiences to access private data collected for one person and then marketed for a very different reason to third parties unconnected with the original transaction. Consent remains the sine qua non of legitimate, commercial data retention.

A person's control of private materials is a matter of autonomy and dignity and should be statutorily safeguarded

---

consumer should buy a product in a well-functioning market: that the product is actually better at doing what it purports to do.").

123. Bambauer, *supra* note 121, at 260.

124. *Id.* at 261.

125. Amanda Taub & Max Fisher, *Where Facebook Rumors Fuel Thirst for Revenge*, N.Y. TIMES, Apr. 22, 2018, at A1; Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 656 (2017).

against commercial exploitation in the United States as it is in Europe. Data subjects should be legally empowered to amend and demand the deletion of commercial data containing private details about their lives and habits.[126] A state appellate judge reviewed the implications of the growing availability of digitally retained data that internet intermediaries obtained for one transaction and then sold to third parties without the subjects' unambiguous consent:

> It is true that mass communication is no longer limited to a tiny handful of commercial purveyors and that we live with much greater access to information than the era in which the tort of invasion of privacy developed. A town crier could reach dozens, a handbill hundreds, a newspaper or radio station tens of thousands, a television station millions, and now a publicly accessible webpage can present the story of someone's private life . . . complete with a photograph and other identifying features, to more than one billion Internet surfers worldwide.[127]

Professor Jeffrey Rosen rejects Article 17 of the GDPR right to erasure ("right to be forgotten") even more vehemently than Bambauer. Rosen would certainly disagree with my effort to have a comparable measure adopted into U.S. law.[128] Rosen writes that the right to erasure "represents the biggest threat to free speech on the Internet in the coming decade."[129] This seems to me to be more than a bit of an overstatement. From where I sit, the risk of Russia, China, or some other adverse sovereign continuing to meddle in future U.S. elections appears to be a much more imminent risk than "the right to be forgotten." Rosen published his condemnation of the "right to be forgotten" in 2012. By the time he made this hyperbolic statement, Russian President Vladimir Putin was shuttering blogging websites that expressed opposition to his regime.[130] In

126. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011).

127. Yath v. Fairview Clinics, 767 N.W.2d 34, 44 (Minn. Ct. App. 2009).

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

129. *Id.*

130. Thomas Grove, *Analysis: Russian Internet Attacks Stifle Political Dissent*, REUTERS (Apr. 13, 2011, 4:03 AM), https://www.reuters.com/article/us-russia-internet-attacks-stifle-political-dissent-idUSTRE73C1P520110413 [https://perma.cc/RGM4

2013, the Chinese government had exploited Google's Gmail service to spy on its citizens and on western commercial enterprises.[131] And Iranian, Belarusian, and Ethiopian security services were incorporating deep packet inspections to snoop out dissent.[132] So, Rosen's claim that the "'right to be forgotten' . . . represents the biggest threat to free speech" is more than a bit misleading.

Rosen does make a good point in arguing that the European Union must provide greater clarification about U.S. businesses' obligations under the GDPR.[133] Anything less could chill free speech. However, unlike Rosen, I am unconcerned that the expense of compliance will impact the bottom line of

---

-MY8Z]; Kevin M. F. Platt, *Russia Blacklists Last Arena of Free Speech*, CGCS MEDIA WIRE (Dec. 3, 2012), https://global.asc.upenn.edu/russia-blacklists-last-arena-of-free-speech/ [https://perma.cc/2CA4-NRQ9]; Andrei Soldatov & Irina Borogan, *The Kremlin's New Internet Surveillance Plan Goes Live Today*, WIRED (Nov. 1, 2012, 6:30 AM), https://www.wired.com/2012/11/russia-surveillance/ [https://perma.cc/HKC7-ZBE8]; Sarah Vrba, *Russians' Internet Privacy Threatened by Putin's Government*, CARE2 (June 27, 2012), https://www.care2.com/causes/russians-internet-privacy-threatened-by-putins-government.html [https://perma.cc/25ZJ-SQ7J].

131. *See* Lolita C. Baldor, *US Looking at Action Against China Cyberattacks*, YAHOO! NEWS (Jan. 31, 2013), https://www.yahoo.com/news/us-looking-action-against-china-231041261.html [https://perma.cc/U68M-UCDJ]; Tom Pullar-Strecker, *Fears Surface Over Chinese Cable*, STUFF: TECH. (Oct. 3, 2011, 8:53 AM), www.stuff.co.nz/technology/digital-living/5720679/Fears-surface-over-Chinese-cable (last updated Mar. 10, 2011, 8:53 AM) [https://perma.cc/XW72-WSKM]; *Top China College Linked to Cyber-Spying Unit*, CNBC (Mar. 24, 2013, 2:04 AM), https://www.cnbc.com/id/100585097 [https://perma.cc/4MXK-2YXB].

132. *Internet Controls in Other Countries: To Each Their Own, China's Model for Controlling the Internet Is Being Adopted Elsewhere*, ECONOMIST: SPECIAL REPORT, Apr. 6, 2013, at 68, https://www.economist.com/special-report/2013/04/06/to-each-their-own [https://perma.cc/MP6Z-M6TY]. Google is returning to the Chinese market, working with that country's government to censor searches as it had prior to 2010. *The World This Week*, ECONOMIST, Aug. 4, 2018, at 5. The rise of autocracies around the globe has only increased the problem. For example, Facebook and Google operating in Vietnam must keep all data of their Vietnamese users in Vietnam, thereby providing the government invaluable surveillance information. *New Data Storage Rules for Facebook and Google as Vietnam Passes Cybersecurity Law*, REUTERS (June 12, 2018), https://www.scmp.com/news/asia/southeast-asia/article/2150345/new-data-storage-rules-facebook-and-google-vietnam-passes [https://perma.cc/6E83-R4TS]. Some autocrats around the world, such as Recep Tayyip Erdoğan in Turkey, are suppressing rather than piggybacking off of online information providers. Benjamin Harvey, *Forget Facebook: Turkey Is Moving to Control All Content*, BLOOMBERG (Mar. 22, 2018), https://www.bloomberg.com/news/articles/2018-03-22/forget-facebook-turkey-is-moving-to-control-all-content [https://perma.cc/BJ7S-23GT].

133. Rosen, *supra* note 128, at 88–90.

companies like Alphabet, Facebook, Twitter, and Yahoo.[134] Congress's concern must be to protect the general welfare of the nation, which is significantly compromised by internet intermediaries' encroachments on the personal dignities of data subjects. The marketing of psychometric profiles by multi-billion-dollar corporations has a substantial effect on the national economy. The collective action problem faced by consumers negatively impacts their abilities to consent to the benefits they can enjoy as audience members of social media, search engines, and other data collection and information companies. They are faced with a plethora of inaccurate, false, and manipulative commercial advertisements that are difficult to distinguish and control because the United States lacks adequate privacy protections.[135] Internet intermediaries sell profiles with tens of thousands of data points to third parties without giving consumers adequate notice and control over the resale of their data.

Internet technology companies have sometimes hidden their data sales to third parties behind excuses of technological complexity to avoid regulators' demands. For example, Yahoo claimed that it could not comply with a French court order to prevent Nazi paraphernalia from being sold on its website to users with French internet addresses.[136] A follow-up expert report later revealed that the company would likely "account for 90% of French Internet users, and the court noted that there was no evidence to suggest that the technical mechanisms to accomplish this filtering would be financially onerous for Yahoo."[137] This is not to say that there will be a quick fix to all foreseeable software puzzles. But the importance of monitoring and enforcement is as critical in the United States as it is in the European Union because of the global nature of privacy issues surrounding new technologies. The foreseeable monetary

134. *Id.* at 88 ("The right to be forgotten could make Facebook and Google, for example, liable for up to two percent of their global income if they fail to remove photos that people post about themselves and later regret, even if the photos have been widely distributed already.").

135. *See supra* text accompanying note 111.

136. Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1184–86 (N.D. Cal. 2001), *rev'd*, 379 F.3d 1120 (9th Cir. 2004), *reh'g en banc granted*, 399 F.3d 1010 (9th Cir. 2005).

137. Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS 261, 268 (2002).

outlay for developing software should not gainsay the convincing arguments for greater consumer control of personal data.

To be clear, I am not advocating that data subjects be granted unbridled control over materials held by digital data commodifiers. Journalistic, historical, literary, artistic, and other matters in the public domain are invaluable to the marketplace of ideas and should be fully protected under the First Amendment. Law enforcement needs are more complex. Data subjects should certainly have a right to expunge arrest records that did not lead to convictions and even misdemeanor records. However, data informing the public of felony convictions, conspiracy, terrorism, and on-going police investigations are better retained to aid in law enforcement. Take as an illustration the role of stored data in unraveling the Boston Marathon bombing of 2013: the terrorists' radical online profiles provided investigators with clues that helped uncover motives and criminal activities.[138] The GDPR provides a model for this nuance as well, exempting companies from having to comply with erasure requests and requirements when the data is retained for national security, defense, public safety, or similar objectives.[139] Corporate initiatives to grant online consumers greater autonomy to purge photographs, delete mistakes and defamations, or erase blog posts should be treated differently. The latter are matters of personal profiles, not public information protected by the First Amendment. The right to privacy should be balanced against listeners' consumer liberty to purchase or otherwise commercially acquire data through ISP servers, search engines, or social networks. The intermediate standard of free

---

138. Press Release, FBI, 2011 Request for Information on Tamerlan Tsarnaev from Foreign Government (Apr. 19, 2013) (https://archives.fbi.gov/archives/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government) [https://perma.cc/HSL8-GU6V]. There is much that could be said here about the potential for police abuses of private information. That discussion would, however, be outside the scope of this Essay, which deals with commercial liability. The literature on national security and privacy on the internet is too vast to tackle in this Essay. *See, e.g.*, David M. Howard, *Can Democracy Withstand the Cyber Age?: 1984 in the 21st Century*, 69 HASTINGS L.J. 1355 (2018); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570 (2017); Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133 (2017); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 542 (2013); Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513 (2014).

139. GDPR, *supra* note 1, at 5.

speech review provides judges with the analytical model needed to evaluate whether the legislature chose narrowly tailored means to achieve the important goal of safeguarding consumer privacy while retaining the liberty that allows for robust, open, and deliberative communications on the internet.[140]

The libertarian bent in U.S. free speech doctrine[141] renders it unlikely that a federal statute comparable to the GDPR will pass here in the near future. The emphasis on speech above privacy in the United States, however, does not gainsay the value of regulating commercial entities that intrude into human data subjects' privacy by indefinitely storing their data and indiscriminately selling it to commercial third parties.

CONCLUSION

The newly enforceable GDPR aims to advance people's "peace and liberty and promot[e] democracy on the basis of the fundamental rights."[142] The United States should follow the EU's lead by recognizing a fundamental right to data privacy as essential to the "well-being of individuals."[143] In keeping with this premise, data subjects should retain significant control over their private information. Internet intermediaries should not only be contractually bound by privacy terms and conditions—as things currently stand in the United States—but also by comprehensive privacy regulation, as is the case in the EU. To achieve these reforms, the United States will need to be more systematic in its privacy regimen, instead of sticking to its current patchwork of unrelated privacy statutes.[144]

---

140. *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 507 (2010) ("The *harm* dimension of the privacy map is important because the ultimate goal of any law, policy, or practice aimed at protecting privacy in the age of the maturing Internet is to deal with actual harms suffered by individuals online."); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1649 (2003) (asserting that "two vitally important and often conflicting goals of Internet regulation" are "first, to allow Internet users to enjoy as much freedom as possible to do as they wish online, and, second, to protect the privacy and security of Internet users and their data").

141. *See supra* text accompanying notes 6 and 55.

142. Directive 95/46/EC, 1995 O.J. (L 281) 31 (EC), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF [https://perma.cc/DVD2-BN9E].

143. *Id.*

144. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012); Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 (2012); 18

None of this is to say that public entities, newspapers, libraries, bookstores, art dealers, or any other contributors to dialogue, culture, and the arts must abide by commercial erasure requirements. And as we saw earlier, the GDPR does not extend to core free speech categories. Rather, I have argued for the need to limit the retention, resale, and analysis of private data collected for specific, commercial reasons. Moreover, users should have control to grant or withdraw consent from the sale of information to third-party vendors. Internet audiences are placed in a commercial panopticon, where third parties keep track of their whereabouts and daily activities. Internet intermediaries' intrusion into the personal lives of data subjects has a substantial effect on the national economy; therefore, federal legislation is in order. Firms have gone so far as to rely on private data to impact deliberative democracy, as was the case during the 2016 U.S. elections.[145] Congress should safeguard consumers' autonomy to maintain control over data that have substantial effect on interstate markets in the aggregate.

Without a regulation requiring internet firms to periodically purge their records, they retain details that are not only useful for commercial audiences but at times are also misleading, defamatory, harassing, propagandistic, and inciteful. Audience members are not simply informed on the internet, they are also commodified there. Without a comprehensive federal

---

U.S.C. §§ 2510–2522 (2012); 18 U.S.C. §§ 2701–2712 (2012) (prohibiting various forms of consumer information compromise by internet and other service providers); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2012); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C. (2012)) (protecting against wrongful disclosure of consumers' private health information); 26 U.S.C. § 6103 (2012) (requiring protection of consumer privacy in tax returns); Privacy Protection Act of 1980, 42 U.S.C. § 2000aa; 47 U.S.C. § 230 (2012); Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521–73 (2012) (requiring protection of cable subscriber privacy); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1831–52 (2010) (discussing the use of traditional torts to obtain redress for privacy infringements on the internet); *State Laws Related to Internet Privacy*, NAT'L CONF. STATE LEGISLATURES (July 25, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/NV8Z-6BQR] (listing and providing hyperlinks to seventeen states' privacy laws).

145. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/CYQ5-U5YU].

statute, U.S. digital consumers are left with virtually no recourse against the black box of data collection. The GDPR provides an excellent model for emerging U.S. policy. With the growth of technology, commercial surveillance will likely increase. Regulatory oversight is needed to provide stronger consumer protections in the digital world, where revealing psychometric profiles are for sale. As things currently stand in the United States, firms can indefinitely retain data and sell it to third parties, even without the data subject's unambiguous, free, and informed consent. Safeguarding the right to erase commercial activity, once it is no longer relevant to the initial transaction for which it was uploaded to the internet, augments consumer control over personal information. The GDPR codified that legal framework. Congress should follow suit by relying on its Commerce Clause authority to empower data subjects' quest for privacy.