THE RIGHT TO ERASURE: PRIVACY, DATA BROKERS, AND THE INDEFINITE RETENTION OF DATA

Alexander Tsesis[*]

INTRODUCTION

The world moves swiftly ahead on the digital platform. The Internet is a place for disseminating information and browsing alone. The screen between publically available information and private data is not, however, as opaque as users might expect. Under current U.S. law, online businesses can track private users without their being aware of the extent to which websites monitor conduct, aggregate it with other personal details, create marketing profiles, and sell the cumulative character sketches to third parties.[1] *The concept of informed consent is often misleading on websites with policies that are written for lawyers and difficult to understand by ordinary Internet users.*[2] *Even when web-based shoppers permit corporate use of their information, they have a very limited ability to ascertain how the businesses will trade, manipulate, and bundle*

---

* Professor of Law, Loyola University Chicago School of Law. I benefited from discussions and written comments on drafts from Alexander Brown, Laura B. Byrne, Richard Delgado, Andrew Epstein, Helen Norton, Richard K. Quinn, Joel Reidenberg, Matthew Sag, Alexandra Roginsky, Olivier Sylvain, and Spencer Waller.

1. *See, e.g.*, Julia Angwin, *The Web's New Goldmine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/news/articles /SB10001424052748703940904575395073512989404 (discussing the ability of private companies to compile information based on an individual's web-browsing preferences, the prevalence of such activity, and the fact that such information is being bought and sold on stock-market-like exchanges); Kashmir Hill, *Verizon Very Excited that It Can Track Everything Phone Users Do and Sell that to Whoever Is Interested*, FORBES (Oct. 17, 2012, 1:46 PM), http://www.forbes.com/sites/kashmirhill/2012/10/17/verizon-very-excited-that-it-can-track-everything-phone-users-do-and-sell-that-to-whoever-is-interested (discussing Verizon's decision to mine user data and sell it for use in "business and marketing reports"); *see also* Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25, 31 (2013) (comparing attitudes on modern data collection in the United States to early frontier attitudes rewarding risk in a lawless atmosphere and concluding that outside of highly regulated industries such as healthcare and finance, unfettered data access and use is encouraged absent demonstrable harm).

2. *See* STEPHEN BREYER, ACTIVE LIBERTY: INTERPRETING OUR DEMOCRATIC CONSTITUTION 69–70 (2005) (writing that "[c]onsent forms can be signed without understanding," making for constructive rather than actual consent).

personal data. Consumers and researchers are often at the mercy of technology they only partially understand, with little they can do to prevent third parties from acquiring and then using sophisticated algorithms to connect details about their online habits with personal—and sometimes embarrassing—information on family, health, and relationship histories.[3]

This Article scrutinizes invasive cyber business practices and advocates passage of the proposed European Union right to erasure. The proposed regulation would prevent the indefinite storage and trade in electronic data, placing limits on the duration and purpose for which businesses could retain it.

The current U.S. consent-based privacy regime allows merchants, databanks, and other electronic aggregators to decide on the data's future uses.[4] Once individuals have divulged online details about their lives, they are often powerless to prevent its dissemination to others whose identity they do not know and whose interests are obfuscated in an almost impenetrable cloud of proprietary secrets. Once divulged on the Internet, private facts about persons' preferences, aversions, job and shopping patterns, and plans are commodifiable at the initiative of profit-seeking corporations with sophisticated business models designed to convert mundane and intimate data, alike, into marketing strategies.

European norms, on the other hand, place more stringent limits on the retransmission and retention of private data. The European Union has demonstrated a greater concern about consumer control over the future uses of their data.[5] Unlike the United States, which tends to concentrate its efforts against state surveillance, European

---

3. JOSEPH TUROW ET AL., RESEARCH REPORT: CONSUMERS FUNDAMENTALLY MISUNDERSTAND THE ONLINE ADVERTISING MARKETPLACE 2–3 (2007), *available at* http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf (finding that 85% of survey participants rejected a "common online advertising model when it [was] explained in simple terms").

4. *See supra* note 1. The opposite presumption applies in Europe. *See* Directive 95/46/EC, of the European Parliament and of the Council, pmbl. 47, 1995 O.J. (L 281) 31, 36 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML ("[T]he controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services . . . .").

5. *See* 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) ("[T]he inherent information privacy value to consumers of having their sensitive personal data protected is adequate to justify EU regulation of sensitive personal data. This leads to different and broader information privacy regulation in the EU as compared to the United States.").

countries have enacted more rigorous regulations to safeguard personal information against corporate abuses.[6]

In light of challenges that consumers throughout the world face, this Article argues that protecting privacy interests of data subjects requires regulation on the length of time and purposes for which businesses can retain electronic information. As matters currently stand in the United States, persons transmitting personal content on the Internet have minimal say in controlling its future manipulation by vendors and third parties. While businesses have legitimate reasons to use data in their day-to-day operations, a statutorily defined expiration period is necessary to preserve the data subjects' dignitary and autonomy rights. Consumer-oriented legislation should prevent indiscriminate capitalization of data initially divulged for specific transactions, such as making purchases or engaging in social networking, but later bundled by third parties for unrelated purposes.

Part I of this Article describes the many forms of data mining that organizations engage in to track online and offline behaviors. The practices are particularly pervasive on social media, which present themselves as platforms for interpersonal communications but also market and trade personal profiles to third parties. Subjects currently have few options, even if they bethink the decision to make information public. Part II evaluates how Internet architecture leaves personal data vulnerable to snooping and surveillance. Part III elaborates on European data regulations and compares them to current U.S. self-help controls. It further argues for adoption of the EU's right to erasure initiative and discusses the likelihood of its enforcement in the United States.

---

6. *See id.* at 454 ("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."); 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."); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1342–51 (2000) (discussing different conceptions of privacy predicated on democratic theories); Eva Dou, *Internet Privacy and the "Right to Be Forgotten,"* REUTERS (Mar. 17, 2011, 11:17 AM), http://www.reuters.com/article/2011/03/17/us-eu-internet-privacy-idUSTRE72G48Z20110317 ("Europe and the United States have traditionally differed on privacy issues, with the EU taking a stronger regulatory approach and U.S. officials more mindful of the need to balance entrepreneurship and business demands with data protection.").

I. INTERNET TRANSACTIONS GONE ASTRAY

While profit maximization is a healthy component of competitive markets, regulation is necessary when the quest for wealth maximization has significant, negative repercussions on consumer privacy and autonomy.[7] Competition requires some degree of firm secrecy, especially in the maintenance of customer accounts. Corporate secrecy can benefit consumers when it helps protect their information, but government intervention is warranted when persons using online services become subjected to an almost unlimited trade in their data. Consent for limited use of data is not a license for its viral spread. Lack of transparency about how companies, especially data brokers, transact in customer information often limits consumers' control over data in ways that cause significant harms to reputation and privacy.[8] Consumers are severely handicapped when information they fill out to complete Internet transactions or that they intend to share only with friends on social media is then resold in the United States or elsewhere

---

7. See Maurice E. Stucke, *Should Competition Policy Promote Happiness?*, 81 FORDHAM L. REV. 2575, 2626–29 (2013), for a discussion of values to consumer protections centered on autonomy and other individual values that are not centered on economic efficiency, arguing for the development of competition policies that will consider "quality-of-life factors (such as individual freedoms, autonomy, environmental protection, and democracy)," not simply surplus maximization. *See also* Graeme B. Dinwoodie & Mark D. Janis, *Confusion over Use: Contextualism in Trademark Law*, 92 IOWA L. REV. 1597, 1625 (2007) ("If we expand the value system of trademarks beyond the scriptures of economic efficiency, we may find an instrumental role for trademark law in preserving real consumer choice and enhancing consumer autonomy."); David G. Owen, *The Moral Foundations of Products Liability Law: Toward First Principles*, 68 NOTRE DAME L. REV. 427, 463–65 (1993) (discussing products liability law in the context of autonomy, equality, and communitarian theory).

8. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 14 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (calling Congress to pass targeted legislation on data brokers, who "compile data for marketing purposes," to "(1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain"); *see also id.* at 68 (defining data brokers as "companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud"); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1957 (2013) (discussing how data brokers, like Acxiom, Google, and LexisNexis, combine various data points about buying habits and web-surfing patterns and sell the information to various marketing sources).

without any input about what third parties can purchase mundane and intimate details about their lives.

Corporate manipulation of private information has increased exponentially with the development of algorithmic software for gathering, packaging, and analytically harvesting data that consumers have provided, without remuneration, to merchants and social networks.[9] Popular companies like Facebook, Amazon, and Google can retain users' data indefinitely and sell it to other companies.[10] Without knowing what use companies are making of their information, consumers are unable to delete, alter, or move anything previously divulged, be it a mistake, misstatement, embarrassing photograph, or whatnot. Data-processing companies thereby gain far greater control over uploaded files, tweets, and blog postings than the person who posted them because U.S. law does not allow him to demand the companies not use it in marketing. Without robust regulation about the use and transfer of personal profiles, commodifiers of data have free rein to augment their worth through privacy eroding practices.

A. Technology of Transmission and Storage

Privacy concerns on the Internet differ from those associated with traditional publishing. The Internet TCP/IP protocol is built to allow cookies of information to be left on users' computers with or without their knowledge.[11] Cookies are bits of information sent from websites to the computers accessing them.[12] Placement and retention of cookies allows the source servers to retrieve information, often for commercial purposes, to expedite exchanges of information.[13] Unless users clear cookies, they could remain lodged in the machine indefinitely. Since most Internet browsers by default receive cookies and consumers typically do not know how to

---

9. Siraj Datoo, *Rapid Development in Big Data Analytics Has Led to Increased Investment*, THEGUARDIAN (Nov. 22, 2013, 10:55 AM), http://www.theguardian.com/news/2013/nov/22/rapid-development-in-big-data-analytics-has-led-to-increased-investment.

10. *Amazon.com Privacy Notice*, AMAZON, http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496 (last updated Mar. 3, 2014); *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last updated Nov. 15, 2013); *Privacy Policy*, GOOGLE, https://www.google.com/intl/en/policies/privacy/ (last modified Dec. 20, 2013).

11. *See* Alexander Tsesis, *Hate in Cyberspace: Regulating Hate Speech on the Internet*, 38 SAN DIEGO L. REV. 817, 829–31 (2001) (describing the technical aspects of Internet transmission).

12. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 274 (11th ed. 2003) (defining "cookie" as "a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a website server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited)").

13. *See* SHELLEY POWERS, LEARNING JAVASCRIPT: ADD SPARKLE AND LIFE TO YOUR WEB PAGES 221 (2009).

prevent companies from lodging them on their computer, by visiting sites consumers become subject to clandestine surveillance.[14] The JavaScript program then allows administrators of websites to analyze users' hard drives while they view web page contents by reviewing data deposited on cookies that were embedded during the subjects' earlier site visits.[15] Without any law forcing the deletion of the information, the consumer becomes subject to the whim of commercial data mining.

Even more reason to consider the passage of a legal right to be forgotten and erasure is the substantial difficulty of removing, or even being aware of, all tracking devices and specialized HTTP packets. "Zombie cookies," also known as "Flash cookies," are larger collections of information relying on the Adobe software and preventing users from blocking them through web browsers' privacy controls.[16] Preventing the retention of Flash cookies through regulation rather than simply self-help is particularly important because they can be placed and indefinitely monitored by commercial venders without the subjects' knowledge.[17] In either format, those tidbits of information are added to the user's profile. The more information stored, the more valuable for the gathering source. Even where cookies are disabled, some companies, like Google Chrome, track consumers' entire viewing history by seeking electronic permission to install a seemingly innocuous software that allows for detailed tracking.[18]

Deep packet inspection is another method for tracking. It enables Internet Service Providers ("ISPs") to look not only at who

---

14. *See* Molly Jennings, *To Track or Not to Track: Recent Legislative Proposals to Protect Consumer Privacy*, 49 HARV. J. ON LEGIS. 193, 194 n.10 (2012) ("Although most web browsers allow their users to disable cookies, some websites do not work without them, leading consumers to avoid such blanket protections."); *see also* Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 291–92 (2012) (discussing methods used by "thousands of websites" to unblock "cookies that consumers ordinarily would not receive" because of how they accidently set their browsers).

15. MAMTA BHUSRY, E-COMMERCE 99 (2005).

16. Ryan Singel, *Privacy Lawsuit Targets Net Giants over 'Zombie' Cookies*, WIRED (July 27, 2010, 4:06 PM), http://www.wired.com/threatlevel/2010/07/zombie-cookies-lawsuit/.

17. *See* John Herrman, *What Are Flash Cookies and How Can You Stop Them?*, POPULAR MECHANICS (Sept. 23, 2010, 5:20 PM), http://www.popularmechanics.com/technology/how-to/computer-security/what-are-flash-cookies-and-how-can-you-stop-them (explaining that Flash cookies are stored separately from other cookies and will not be deleted when other cookies automatically are); *What Are Local Shared Objects?*, ADOBE, http://www.adobe.com/security/flashplayer/articles/lso/ (last visited Jan. 20, 2014) (giving an explanation of Flash cookies and how they operate).

18. Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 11–12 (2011).

sent what to whom but the actual content of the messages.[19] This method enables ISPs to record the content of users' search queries, their social media activities, and even text portions of personal emails.[20] Among the newest forms of tracking technology, still in its developmental stages, is "fingerprinting," which enables hosts to run JavaScript bench markers to circumvent conventional security methods, like using proxy servers to obfuscate identity or opting out of cookie placement.[21] Fingerprinting tracks users "[b]y collecting the properties of PCs, smartphones and tablets including their screen size, the software versions they're running and which plug-ins are installed"[22] and is typically run in an effort to circumvent European and U.S. laws on the propagation of cookies.[23] The proposed European "right to erasure," about which I elaborate in Subpart III.B of this Article, would prevent indefinite data mining.

---

19. *Id.* at 12–13 & n.62 ("[D]eep packet inspection devices are capable of not only reading the information on the outside of the envelope but the letter inside during the course of delivery.").

20. *See id.*; Steven R. Morrison, *What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 253, 267 (2011) ("The process of deep-packet inspection is similar in effect to what Google does, but enables ISPs (as opposed to Google, which is not, strictly speaking, an ISP) to look closely into a computer user's Internet activity, including email content."); Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1438–39 (discussing the depth with which ISPs can access all of a user's browsing history, including through the use of deep packet searching of content, to include "instant message, video download, tweet, Facebook update, file transfer, VoIP conversation, and more"); Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1769 (2013) ("[M]ajor ISPs routinely sample the traffic passing through their network and use deep packet inspection (DPI) to examine it for security threats."). A lawsuit filed in the United States District Court for the Northern District of California claimed that Google had "intercepted, read and acquired the content of [private] email [messages] for the purposes of sending an advertisement relevant to that email communication to the recepient [sic], sender, or both" in violation of California's privacy laws and federal wiretapping statutes. *In re* Google Inc., No. 13-MD-02430-LHK, 2013 WL 5423918, at *1 (N.D. Cal. Sept. 26, 2013). Google not only searches the content of persons with Gmail accounts who have agreed to its terms of usage but also that of persons without Gmail accounts sending emails to those with that service. *Id.* at *12.

21. *See* HONG KAING ET AL., USER TRACKING: PERSISTENT COOKIES AND BROWSER FINGERPRINTING 2 (2013), *available at* http://cs.gmu.edu/~yhwang1/INFS612/2013_Spring/Projects/Final/2013_Spring_PGN_5_final_report.pdf (discussing how fingerprinting can be used to track users even when those users believe they have deleted all cookies from their computers).

22. Ian Barker, *Websites Use Device Fingerprinting for Secret Tracking*, BETANEWS (Oct. 11, 2013), http://betanews.com/2013/10/11/websites-use-device-fingerprinting-for-secret-tracking/.

23. GUNES ACAR ET AL., FPDETECTIVE: DUSTING THE WEB FOR FINGERPRINTERS 1 (2013), *available at* www.cosic.esat.kuleuven.be/publications/article-2334.pdf?.

B. *Privacy Online*

1. *Privacy in a Linked World*

Surveillance scholars have traditionally focused on government intrusions.[24] In today's digitized world there is also much to be concerned about regarding private snooping. Because the companies involved in the practice are not state actors, Fourth Amendment doctrine does not bar ISPs, Internet browser companies, retail companies, and search engines from searching and seizing information about private matters.[25] Businesses with Internet platforms regularly gather private information, for which they would require a warrant if they were state actors, run it through algorithms, categorize persons on the basis of predetermined stereotypes, conduct statistical analyses on their data, and formulate business models.[26] Consumers, students, and others on the Internet benefit from this feedback by getting more accurate and personalized returns on searches and advertisements that are integrated into third party websites or that they receive by e-mail.[27] But the benefits of personalized market analysis come with little consumer control over what information is being manipulated for corporate gain. Details about people's lives, shopping habits, relationships, browsing histories, family backgrounds, etc., can easily be retained—without the knowledge of

24. *See, e.g.*, Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21 *passim* (2013) (discussing whether and how the Fourth Amendment applies to usage of new forms of electronic surveillance by police and proposing "a two-part definition of a Fourth Amendment 'search' in a public space"); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1354–55 (2004); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 *passim* (2004) (advocating for legislative, rather than judicial, rules to protect citizens from invasions of their privacy by the government).

25. 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.").

26. *See* Berger, *supra* note 18, at 4 (discussing how data collection and resulting customer profiles can be used for targeting customers' interests).

27. *See* Hana Mujadzic, *Are You Making the Most of Customer Data?*, ABC TECH. & GAMES (Nov. 11, 2013), http://www.abc.net.au/technology/articles/2013/11/11/3888271.htm (discussing customer experience optimizing through the use of collected data).

subjects—in digital databases.[28] With no limit on the length for retention, the data can be systematically augmented for years.

The companies have no obligation under U.S. law to ever delete this information, even when its storage has long outlived any usefulness to a consumer. A person who uses a search engine to find out about high blood pressure might benefit for a time from receiving advertisements on how to get well. Once he gets the condition under control through diet and exercise, however, such advertisements might no longer be relevant. But, for health care insurance companies trying to determine the prior health histories of their clients, it might be worth acquiring customers' Internet search histories. Thus, a conflict of interests exists between the consumer and marketer.

One of the Internet's chief draws is its capacity to facilitate person-to-person contacts and commercial exchanges. But while electronic shoppers view their desired product, with no popup warning, many companies gather viewing patterns, keep track of purchases to identify shopping patterns, and sell shoppers' profiles. Choices consumers make provide clues about who they are. For instance, someone who buys children's products is likely to have his or her own children or, at least, to shop for children in the future; a shopper's sex might be gleaned from products searched and purchased; and someone's medical needs can be discovered by online pharmaceutical transactions.[29] Data mining is not only used by businesses. Political parties, medical researchers, and public entities also exploit clandestinely gathered data to accumulate databanks of private details about targeted parties.[30] Just like purchasers, persons searching for political information or making sense of physical or mental conditions are often unaware of the extent to which their information is collected, disseminated, and

---

28. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 107 (2012) (discussing electronic surveillance and its storage in databases).

29. *See* JOHN WANG, DATA MINING: OPPORTUNITIES AND CHALLENGES 397–98 (2003). Many books are available about how to exploit the data gathered from the collected inputs, allowing entities to use algorithms, statistical models, and evaluative methods to transform raw data by evaluating patterns into manipulable interpretive outputs. *See generally, e.g.*, JIAWEI HAN ET AL., DATA MINING: CONCEPTS AND TECHNIQUES (3d ed. 2012) (providing information on data mining ranging from basic definitions and statistical analysis of data to analytical processing and picking out trends in data); DAVID L. OLSON & DURSUN DELEN, ADVANCED DATA MINING TECHNIQUES (2008) (presenting different approaches to data mining and discussing the value of each approach to businesses); IAN H. WITTEN ET AL., DATA MINING: PRACTICAL MACHINE LEARNING TOOLS AND TECHNIQUES (3d ed. 2011) (discussing both basic and advanced data mining techniques, including basic data mining algorithms and using mined data to predict future trends).

30. *See, e.g.*, Charles Duhigg, *Campaigns Mine Personal Lives to Get Out Vote*, N.Y. TIMES, Oct. 13, 2012, at A1.

sold, and how much of their histories can be traced at a speed only limited by technologies. Marketers or political advisers can also develop strategies by analyzing the viewing and purchasing histories of consumers who have registered on Facebook, Google+, LinkedIn, or Twitter as fans and followers of various enterprises.[31] Without regulations, marketers, government agencies, and data aggregators have commercial incentives to retain the gathered metrics for their own and other companies' marketing plans.

Even data unavailable through public records can be rendered searchable on the Internet. Embarrassing or traumatic scenes that in the past would have been quickly forgotten or would have entered the long-term memories of observers might now be captured on cell phone cameras or Google Glass. Persons who are given to jumping for joy, laughing uproariously, crying and otherwise showing the outward signs of mourning, dancing, or yelling have reason to be concerned that those spontaneous expressions of their personalities can be captured on electronic media and spread through Internet software. A skirt being blown up by the wind or a bikini falling off at a beach, matters for momentary embarrassment, can now become immortalized on web servers. There are also professional costs of the new technology and a sense of empowerment (for some and disempowerment for losers of the propositions), with employers, coworkers, and college admissions counselors increasingly having access to personal, compromising tidbits.[32] Such privacy issues, as I later demonstrate, can only be resolved through regulation, not solely by fictitious consent by consumers who disclose their information with almost no knowledge of where, for how long, and when their private details will be disclosed.[33]

---

31. Carter Hostelley, *Struggling with B2B Social Marketing? Here's What to Do Now*, BUS. 2 COMMUNITY (Jan. 31, 2013), http://www.business2community.com/b2b-marketing/struggling-with-b2b-social-marketing-heres-what-to-do-now-0393764#!sL2Uu (providing advice for strategic online marketing plans).

32. *See, e.g.*, Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, N.Y. TIMES, Nov. 10, 2013, at BU3 (discussing college counselors' uses of online accounts to vet admissions candidates); Russ Warner, *Beware of Legal Threats Social Networks Pose, Blog*, HUFFINGTON POST (Aug. 30, 2013, 12:25 PM), http://www.huffingtonpost.com/russ-warner/beware-of-legal-threats-s_b_3832632.html (writing about employers and college entrance boards use of social network profiles in their decision processes); *see also* Jason R. Finkelstein, *New Jersey Social Media Privacy Bill Signed into Law*, EMP. L. MONITOR (Sept. 4, 2013), http://www.employmentlawmonitor.com/2013/09/articles/employment-policies-and-practi/new-jersey-social-media-privacy-bill-signed-into-law/ (providing information about a New Jersey law prohibiting potential employers from require job candidates to provide social media identifications and passwords).

33. *See infra* Subparts III.A–B.

Internet architecture might soon facilitate unprecedented snooping. Face recognition technologies are improving and software engineers are tinkering with existing software limitations by adjusting for aging and differences in shadowing.[34] It is now foreseeable that in the not-too-distant future, persons will be able to use face recognition technology to stalk others through the lenses of public cameras placed on streets for very different public purposes.[35] Before the advent of the Internet, gossip about private persons tended to be localized, but streaming media have changed dynamics of human interactions. Photos and videos captured in public places, where it is perfectly legal to obtain them, can detrimentally affect others' lives even though their dissemination does not constitute defamation or any other tort, including intrusion to seclusion or invasion of privacy.[36] Enforcing a maximum time for retaining information would diminish the risks of harms persons can experience from third party retention of their information.

Cellcam vigilantism and snooping have become accepted and even lauded as an avenue for vengeance.[37] YouTube has an array of videos of embarrassing altercations that took place at sports events, which might have been played down but that the buffoonery is almost permanently electronically preserved,[38] there to be viewed by boyfriends, girlfriends, employers, children, and the many other people whose glare is uninvited. Without legislative intervention, these ephemeral lapses in judgment can become permanent stains on persons' records, potentially affecting employment, church membership, and relationships.

Persons who are the objects of those videos lack any legally cognizable control over their content and its availability. At a recent

---

34. So Ra Cho et al., *Face Recognition Algorithm for Photographs and Viewed Sketch Matching Using Score-Level Fusion*, 9 INT'L J. ADVANCED ROBOTIC SYS. 1, 1–3 (2012) (discussing new research methods to overcome shadows and other anomalies in photographs to improve facial recognition).

35. See Jeffrey Rosen, *Introduction: Technological Change and the Constitutional Future*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 1, 1 (Jeffrey Rosen & Benjamin Wittes eds., 2011), for a chilling description of a world where face recognition provides users the means of tracing someone's steps and then copying the image into Facebook's or Google's databases to identify and find details about her life. See also, for example, *Alaska Webcams*, ALASKA MINING & DIVING SUPPLY, INC., http://www.akmining.com/webcams.htm (last visited Jan. 19, 2014), for one list of publicly available cameras located in Alaska.

36. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

37. *See, e.g.*, Victoria Woollaston, *The Bunny Boiler App: Spy Software Lets You Track a Partner's Movements, Listen in on Calls and Even Lock Their Phone*, DAILYMAIL (Nov. 28, 2013, 5:43 AM), http://www.dailymail.co.uk/sciencetech/article-2514892/mSpy-app-lets-people-spy-partners-calls-texts-track-them.html (discussing a popularly available application that allows cell phone surveillance among individuals).

38. *See, e.g.*, *Greedy Broad Steals Foul Ball*, YOUTUBE, https://www.youtube.com/watch?v=6locBvdMJtw (last visited Jan. 19, 2014).

Silicon Valley event, Adria Richards, then an employee of the e-mail company SendGrid, took a picture with her cell camera of two men making a "lame" dirty joke, and posted their photo on Twitter along with a reproachful comment.[39] Her post was widely circulated, setting off unexpected results: First, one of the men engaged in the joke was fired; later, SendGrid received so much negative publicity that they fired Richards.[40] A permanent electronic record now exists of this and many other innocuous events that would have otherwise been out of sight and out of mind. With such potentially negative repercussions for so mundane a happenstance, persons might well think twice about exercising their First Amendment rights, diminishing their willingness to express ideas that benefit themselves and society.

Besides the availability of posts uploaded by others, third parties can obtain a wealth of private information by simply asking users who visit websites to register their names, addresses, income levels, and other demographics in a bid to improve user services. While this practice seems innocuous because it initially relies on users to grant implicit or explicit consent for the retention of data, the seeming transparency is a marketing strategy that obfuscates the exploitation of customer data far afield of the initial transactions and outside the consumer's consent. Companies need not stop at the limits of the information users leave on their websites. They can also purchase or share consumer details purchased from other companies. Under the current legal regime for business transactions in the United States, data collection is legal without the subject's consent unless the practice violates a limited number of statutory guidelines for reporting specific facts, such as healthcare records and credit reports.[41] An ISP—like America Online and EarthLink—can consolidate more information about users than their families and closest friends know and even more than the subject may remember.

Securing privacy is not solely important on a personal level. Business corporations, charities, universities, financial institutions, libraries, and many other nongovernmental entities store an enormous amount of data that patrons may not want divulged to third parties.[42] Even when that information is not being mined,

---

39. David Streitfeld, *Google Glass Picks Up Early Signal: Keep Out*, N.Y. TIMES, May 6, 2013, at A1.

40. *Id.*

41. See *infra* note 221 for a list of federal privacy statutes. *See also* Michael Margolis, *E-Government and Democracy*, *in* THE OXFORD HANDBOOK OF POLITICAL BEHAVIOR 765, 778 (Russell J. Dalton & Hans-Dieter Klingemann eds., 2007) (explaining methods for extracting information from consumers via websites).

42. TRINA J. MAGI, PROTECTING LIBRARY PATRON CONFIDENTIALITY—CHECKLIST FOR BEST PRACTICES 1 (2006), *available at*

there are concrete privacy concerns at stake regarding their long-term and permanent retention. All servers are prone to hacking attacks and internal, organizational abuses that can severely affect customers and patrons. People share their information to make friends, participate with others in distant communities, create bonds they would not have otherwise been able to forge because of physical separation, seek to profit, pay bills, plan vacations, and engage in many other interactive group relationships. The risk arises when companies share that information and mine it for profit-making schemes over which the subject has no control or knowledge. Regulations empower ordinary users against the corporate data retention.

The ease with which information can be shared over the World Wide Web—across borders with friends, acquaintances, and complete strangers—is unparalleled at any point of history. Cyberspace communication raises unique problems for those subjects of communication who wish their information to be circulated only for a limited purpose and not distributed to third parties without prior permission. For them, statutory intervention is necessary because U.S. constitutional doctrine grants corporations great latitude about acquiring, exploiting, and disseminating data.[43] The First Amendment protects corporations and private parties who transmit information that they gathered about people or businesses engaged in social networking and other web surfing.[44] There are no constitutional limits in the United States on how long that information can be retained.[45] Indeed, in 2011 the Supreme Court

---

http://www.webjunction.org/content/dam/WebJunction/Documents/illinois/Confidentiality_Best_Practices.pdf (discussing the vast array of information now collected by libraries); Marc Parry, *Please Be eAdvised*, N.Y. TIMES, July 22, 2012, at ED24 (discussing how colleges store students' browsing data); Brad Stone, *Drawing a Bead on Debtors*, N.Y. TIMES, Oct. 21, 2008, at B1 (discussing how financial institutions utilize data mining); Zachary Karabell, *Americans' Fickle Stance on Data Mining and Surveillance*, ATLANTIC (June 14, 2013, 11:23 AM), http://www.theatlantic.com/national/archive/2013/06/americans-fickle-stance-on-data-mining-and-surveillance/276885/ (discussing the types of data exploited by corporations); Vanessa Small, *Charity Works: How Crunching Big Data Can Save a Child*, WASH. POST (Sept. 15, 2013), http://www.washingtonpost.com/business/capitalbusiness/charity-works-how-crunching-big-data-can-save-a-child/2013/09/13/33551420-1bfc-11e3-8685-5021e0c41964_story.html (discussing information charities store about the individuals whom they serve).

43. Slobogin, *supra* note 25, at 328–30.

44. Timothy Zick, *Territoriality and the First Amendment: Free Speech at—and Beyond—Our Borders*, 85 NOTRE DAME L. REV. 1543, 1573 (2010) ("[T]he First Amendment would likely protect one private party from sharing information with another private party—even if there was some possibility that the information might be used for evil or illegal purposes.").

45. The ACLU obtained information from the U.S. Department of Justice indicating that some phone carriers never fully divest themselves of user data. *See Cell Phone Location Tracking Request Response-Cell Phone Company Data*

struck down a Vermont statute on First Amendment grounds that it had prohibited pharmacies from sharing prescription information with pharmaceutical companies.[46] For the most part, therefore, in the United States consumers must rely on the goodwill of companies, whose interests are separate from consumers, to advance dignitary and autonomy interests in privacy.

2. Social Networking

The growth of social networks, like Facebook, Twitter, MySpace, and Google+, has added layers of complexity to the legal understanding of privacy. These social spaces are platforms for commerce and person-to-person interactivity on a scope never imagined before the World Wide Web made cross-border communications within reach of ordinary people. Millions find social media to be a reliable, and indeed often necessary, means for contacting acquaintances, staying close to family, maintaining professional links, or sharing all manner of intimate and mundane information with the world at large.[47] Given the extent to which electronic communications have become part of people's lives, it is no wonder that companies systematically harvest personal profiles. The situation is somewhat different here than that discussed in the previous Subpart of this Article on business transmissions and ISP contacts because people typically post materials about themselves on social networks with the specific purpose of having others see and read them. Concerns arise when companies clandestinely gather and disseminate data from social media without users' permissions and often against their stated desires.[48] Moreover, even the unwarranted retention of data posted voluntarily, especially by children and teenagers, limits the autonomy of users, favoring, instead, the commodification interests of data controllers.

As of 2013, 50% of the U.S. population between the ages of thirteen and one hundred use Facebook services, amounting to

---

Retention Chart, AM. CIV. LIBERTIES UNION (Aug. 2010), https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

46. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2660, 2665, 2672 (2011).

47. *See Social Networking Fact Sheet*, PEW RES. INTERNET PROJECT (Dec. 27, 2013), http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx.

48. *See* Nick Eaton, *Suit: Amazon Fraudulently Collects, Shares Users' Personal Info*, SEATTLEPI (last updated Mar. 2, 2011, 10:00 PM), http://www.seattlepi.com/business/article/Suit-Amazon-fraudulently-collects-shares-users-1040886.php (discussing a class action law suit against Amazon claiming the company clandestinely gathered information on patrons by using Adobe Flash Player cookies). For more information about the underlying lawsuit, see generally *Del Vecchio v. Amazon.com, Inc.*, No. C11-366RSL, 2012 WL 1997697 (W.D. Wash. June 1, 2012).

roughly 168 million accounts.[49] Three countries—Brazil, India, and Indonesia—have over 50 million users.[50] People living in a host of other countries also have tens of millions who connect through Facebook, with a whopping total of about a billion users.[51] Twitter is not quite as populated, and yet its numbers are enormous, with 500 million accounts worldwide;[52] even though the popularity of MySpace has waned, in November 2012 the site experienced a growth of over 10% with 27.7 million visitors;[53] and Google+, a newer social networking service, has about 300 million registered users.[54]

Facebook, for one, has been remarkably successful in convincing users to publically divulge information. Its News Feed service functions to share the videos, photographs, and stories that a user has viewed and makes that information available to a select group of others.[55] Facebook tagging allows members of the network to reveal the chronological steps of their daily lives.[56] Without opting out of these features, users essentially tell others where they have been, to whom they have spoken, and the many activities they enjoyed or disliked. Beyond immediate curiosity many posts—such as those relating what food a person ordered at a restaurant or what running route she took—are too mundane for anyone to remember, but electronic marketing companies store and analyze these self-

---

49. Tom Webster, *Facebook Achieves Majority*, EDISON RES. (Mar. 24, 2011), http://www.edisonresearch.com/home/archives/2011/03/facebook_achieves_majority.php.

50. Maximillian H. Nierhoff, *Facebook Country Stats January 2013—Brazil and India Are Adding Millions*, QUINTLY, http://www.quintly.com/blog/2013/01/facebook-country-stats-january-2013-brazil-and-india-are-adding-millions/ (last visited Mar. 2, 2014).

51. *See* Andrew Moran, *Social Media Landscape Adds Another Outlet to the Mix: Slingjot*, DIGITAL J. (Jan. 15, 2013), http://digitaljournal.com/article/341364. Facebook estimates that one billion people use its service actively. *See One Billion People on Facebook*, FACEBOOK (Oct. 4, 2012), http://newsroom.fb.com/News/457/One-Billion-People-on-Facebook.

52. Marissa McNaughton, *Social Networking Stats: Facebook Nears Global Domination, #RLTM Scoreboard*, REALTIME REP. (Jan. 4, 2013), http://therealtimereport.com/2013/01/04/social-networking-stats-facebook-nears-global-domination-rltm-scoreboard/.

53. Kevin Sablan, *MySpace Continues to Grow as Facebook Dips Again*, ORANGE COUNTY REG. (last updated Aug. 21, 2013, 1:17 PM), http://www.ocregister.com/articles/facebook-382036-new-myspace.html.

54. Alistair Barr, *Google's Social Network Sees 58% Jump in Users*, USA TODAY (Oct. 29, 2013, 6:58 PM), http://www.usatoday.com/story/tech/2013/10/29/google-plus/3296017/.

55. *What Is News Feed?*, FACEBOOK, http://www.facebook.com/help/210346402339221/ (last visited Feb. 8, 2014).

56. *What Is Tagging and How Does It Work?*, FACEBOOK, http://www.facebook.com/help/124970597582337 (last visited Feb. 8, 2014).

reports.[57] While a person may be perfectly happy posting the information, she may later reconsider the post. Under current law, Facebook is under no obligation to erase that data from its servers, even if a user deletes her profile.[58] By keeping their vast data troves out of the public's eye, while maintaining them on servers and analyzing them through complicated algorithms, firms create the image of facilitating advertising and sale to government agencies without drawing much attention to the commercial value of providing free services.

When the News Feed function first appeared, many users expressed outrage, but it has now become an accepted feature.[59] To Facebook's credit it allows users to limit which friends have access to the News Feed eed or tagged items, but that does not prevent the company from retaining complete profiles for its own business, and members cannot prevent Facebook from gathering valuable data.[60] The level of detail maintained on each person is far greater than an ordinary store's customer records. In September 2013, the Federal Trade Commission ("FTC") began to investigate a change to Facebook's written disclosure, explicitly informing its users of a heretofore clandestine initiative to collect for advertisement users', including minors', picture profiles, names, and other details such as companies that members indicated they "like."[61]

Revelation of private histories can be a source of embarrassment, acrimony, surveillance, and stalking. In 2010, Google revealed the identity of users posting comments on its Google Buzz feature, a microblogging tool.[62] Then, in 2012, the FTC issued

---

57. Dave Williams, *Connecting the Data Dots on Facebook and Beyond*, ADVERTISING AGE (Sept. 16, 2011), http://adage.com/article/digitalnext/marketers-facebook-audience-data/229244/.

58. *See Information We Receive and How It Is Used*, FACEBOOK, https://www.facebook.com/about/privacy/your-info (last visited Feb. 8, 2014) (stating that information deleted from an active Facebook user's profile may be retained until the account is permanently deleted but also stating that certain account activities will be retained even after the account is deleted).

59. Eric Eldon, *Analysis: Some Facebook Privacy Issues Are Real, Some Are Not*, INSIDEFACEBOOK (May 11, 2010), http://www.insidefacebook.com/2010/05/11/analysis-some-facebook-privacy-issues-are-real-some-are-not/.

60. *See Data Use Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last visited Feb. 8, 2014).

61. *See* Elizabeth Dwoskin, *FTC Probing Facebook's New Privacy Policy*, WALL ST. J., Sept. 12, 2013, at B2.

62. In 2010, the FTC announced a settlement in its action against Google for converting private, personal information of Gmail subscribers into public information for the company's social network service Google Buzz. *See* Theodore C. Max, *Charting a Safe Course in the Perfect Storm of Consumer Privacy Laws*, METROPOLITAN CORP. COUNSEL (May 31, 2011), http://www.metrocorpcounsel.com/articles/13927/charting-safe-course-perfect-storm-consumer-privacy-laws; Grant Gross, *US Lawmakers Ask for FTC Investigation of Google Buzz*, TECHWORLD (March 30, 2010, 6:43 AM),

a $22.5 million fine against Google "for bypassing privacy settings in the Safari browser."[63] And in 2013, Facebook admitted that it had inadvertently exposed the phone numbers and e-mail addresses of six million of its users.[64] Requiring companies to purge the information from their files after an expiration period, as the right to erasure proposes, will diminish the amount of personal detail that can be inadvertently revealed.

Corporations amass treasure troves from people posting intimate details about their daily lives, without making clear what, if anything, will be resold to third parties. Persons using Gmail, for instance, expose the content of their e-mails to Google and ultimately to advertisers.[65] Google has optimized its ability to obtain an enormous record about individuals by asking users to sign into its various services, including Google+, and then interlinking the information to create personalized dossiers.[66] Facebook, too, sells users' personal data—about such things as music preferences, political affiliations, entertainment interests, and hobbies—to companies who are far removed from the "friends" with whom the user may have initially wished to be in contact.[67] Without a limit on the period for which social networks can retain a record of the subject's postings, a private person is almost helpless to prevent the indefinite amassing of data by companies like Acxiom and cannot delete politically charged statements that may put her and her family in danger.

---

http://www.techworld.com.au/article/341341/us_lawmakers_ask_ftc_investigation_google_buzz/. Subsequently, Google agreed to a $22.5 million settlement over an FTC charge alleging that Google violated the earlier settlement with the FTC over the Google Buzz problems, which forbade the company "to misrepresent its privacy policies to consumers." Hayley Tsukayama, *Google Settles FTC Privacy Case for $22.5 Million, Agency's Largest Penalty*, WASH. POST (Aug. 9, 2012, 11:56 AM), http://www.washingtonpost.com/blogs/post-tech/post/google-settles-ftc-privacy-case-for-225-million-agencys-largest-penalty/2012/08/09/e048f6a2-e236-11e1-a25e-15067bb31849_blog.html.

63. David Streitfeld, *Google Concedes Drive-by Prying Violated Privacy*, N.Y. TIMES, Mar. 12, 2013, at A1.

64. *Important Message from Facebook's White Hat Program*, FACEBOOK (June 21, 2013, 4:50 PM), https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766; Michael Rundle, *Facebook Admits Leak of Six Million Email Addresses and Phone Numbers*, HUFFPOST TECH U.K. (June 24, 2013, 8:54 AM), http://www.huffingtonpost.co.uk/2013/06/24/facebook-leak-2013_n_3488908.html.

65. *See* DUNCAN LONG, PROTECT YOUR PRIVACY 148 (2007) (describing how Gmail "employs 'content extraction,' searching through the e-mail for the keywords sold to advertisers").

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

67. *See id.* at 5–6, 39, 189–90, 194 (describing Facebook's methods of collecting and disseminating private information).

Government entities engaged in surveillance have also found a wealth of details about the habits and whereabouts of individuals whom they wish to track without obtaining a warrant.[68] Without adequate oversight, this method of law enforcement easily lends itself to abuse. Indeed, at the hands of 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.[69]

---

68. *See* Cecilia Kang, *Facebook, Microsoft Release Number of Data Requests from Government*, WASH. POST (June 14, 2013) http://www.washingtonpost.com/business/technology/2013/06/14/61a6ff1e-d55c-11e2-a73e-826d299ff459_story.html.

69. 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/ (providing a list of some of the countries that expressly suppress dissent on social media). In Iran, during the brief 2009 uprising, the regime arrested bloggers and online critics for voicing antigovernment sentiments. *See* Peter Goodspeed, *Goodspeed Analysis: The Arab Spring May Have Helped Usher in a New Era of Government Surveillance, Full Comment*, NAT'L POST (Apr. 21, 2012, 1:31 A.M.), http://fullcomment.nationalpost.com/2012/04/21/goodspeed-analysis-governments-could-soon-record-and-store-everything-their-citizens-do-from-birth-to-death/. A human rights expert and UN rapporteur, Ahmed Shaheed, recently detailed how, along with the country's many other human rights abuses (including torture by baton beatings, rapes, sleep deprivation, and public hangings), the Islamic Republic's regime has detained at least nineteen bloggers, condemning four of them to death in January 2012 for "enmity against God" and "corruption on earth." *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. In China, Google discovered that hackers had accessed the personal e-mail accounts of several hundred Gmail users, including "senior [U.S.] government officials . . . , Chinese political activists, officials in several Asian countries, military personnel and journalists." John Markoff & David Barboza, *Hackers from China Hit Gmail, Google Says*, N.Y. TIMES, June 2, 2011, at B1. Pakistan has a record of shutting down Internet communication technologies and banning social networks; moreover, the government has a "record of arresting bloggers and users for political writing and their deaths in captivity." *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/. During the September 2007 monk-led uprising in Burma, the ruling regime censored the posting of videos and other information by blocking access to the Internet. *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; Patricia Maunder, *The Great Firewall of China*, SYDNEY MORNING HERALD (Australia) (Mar. 20, 2008), http://www.smh.com.au/news/web/the-great-firewall-of-china/2008/03/18/1205602389513.html. In 2011, the Syrian government allowed access to users to post messages on Twitter and Facebook, but the country monitored the messages of persons using those accounts to make it easier for officials to track down dissidents. *Government Control of the Internet*, SLAW (Jan. 16, 2013), http://www.slaw.ca/2013/01/16/government-control-of-the-internet/. King Abdullah of Saudi Arabia has

Perhaps even more troubling than the potentially permanent maintenance of consensual posts is that companies also collect data on parties who did not approve of the postings. Photographs with images of third parties—ones whom even the party uploading the documents might not know or, on the other hand, might tag by name—help entities create marketing profiles.[70] Even a photograph of a person who does not use Facebook, has no interest in the services, or might be outright averse to it, can be "tagged" by name to be viewed by friends, enemies, and employers alike.[71] What is more, cookies and other tracking devices are often installed in computers without owners' knowledge and cached on computers.[72] Through cookies technologies clickstream data, a website can track what a person views, how long it is viewed, connect the browsing history to previous search history, and algorithmically develop a profile for marketing new objects to the patron.[73] A website placing cookies on users' computers may be gathering information that it can resell for advertising purposes after having collated a behavioral profile.[74] While users can set their browser setting to reject cookies, placing a complete block on them effectively blocks users' access to many websites that refuse to provide services without accepting the cookies.[75] Once gathered, there is currently nothing requiring companies to delete mundane or embarrassing details that might later resurface and negatively impact the subject's employment or other decisions, even after data have become stale and no longer present an accurate depiction.

The friendship and messaging services not only reveal information about people who disclose it but also about their unwilling friends as well. An empirical study by two computer

---

authorized the police to "crack down hard on dissidents that thrive in the Internet medium." Sreeram Chaulia, *A Pressing Matter*, FIN. EXPRESS, May 7, 2010 at 9, *available at* http://www.sreeramchaulia.net/publications/PressPredators.htm.

70. *See "Liking" Has Consequences*, DETROIT NEWS, Sept. 7, 2012, at A2 (asserting that a deputy was fired for clicking the Facebook like button on the "page of the candidate running against the incumbent sheriff"). A BMW dealership fired a car salesman for posting critical Facebook posts. *Id.*

71. A teacher was suspended after someone posted a photograph of her with a stripper at a bachelorette party, but her employer later reinstated her. Joe Mandak, *Teacher Suspended over Facebook Stripper Photo Settles*, HUFFINGTON POST (Aug. 17, 2010, 11:54 AM), http://www.huffingtonpost.com/2010/08/17/facebook-stripper-photo-c_0_n_685095.html.

72. Hoofnagle et al., *supra* note 14, at 273.

73. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1624–25, 1641, 1645 (1999) (describing how ISPs and websites track users' information).

74. *See* ANDREJ SAVIN, EU INTERNET LAW 213–14 (2013) (describing the technological applications of cookies).

75. *See, e.g.*, Hoofnagle et al., *supra* note 14, at 290 (noting that the popular television-streaming website Hulu requires users to accept cookies in exchange for services).

scientists of 4,080 Facebook profiles determined the sexual orientation of individuals on Facebook, whether or not they disclosed the information on their own, by analyzing the friendship lists of self-identified gay men.[76] This form of backward tracking poses significant privacy concerns for those who do not want that aspect of their lives to be known to strangers who happen upon their profile pages. Discrimination on the basis of same-sex attraction remains high, and the consequences of this information getting into the hands of persons with ill intents might be significant in the workplace and other settings. Twenty-nine states do not include sexual orientation as a protected category in their employment discrimination laws.[77]

Keeping aspects of one's life private for professional or other reasons can be compromised in unexpected ways through social networks. Facebook lacks the financial incentive to disclose the ripple effects of constructing friendship lists or to permanently purge the information from its databanks, even if users choose to later change their profiles. What is more, Facebook's policy of introducing technological innovations through opt-out (rather than opt-in) features means that details of one's life could be revealed by oversight, technological error, or ignorance rather than personal volition.[78] Furthermore, Facebook periodically changes its policies and exposes information that it held confidential under previous

---

76. Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, FIRST MONDAY (Oct. 5, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2611/2302.

77. Twenty-one states and the District of Columbia prohibit employment discrimination on the basis of sexual orientation. *See* CAL. GOV'T CODE § 12940(a) (Deering 2010); COLO. REV. STAT. § 24-34-402(1)(a) (2013); CONN. GEN. STAT. ANN. § 46a-81c (West 2013); DEL. CODE ANN. tit. 19, § 711(a) (West 2013); D.C. CODE § 2-1402.11(a) (LexisNexis 2001); HAW. REV. STAT. § 378-2(1)(A) (1993); 775 ILL. COMP. STAT. ANN. 5/1-102(A) (West 2013); IOWA CODE ANN. § 216.6 (West 2009); ME. REV. STAT. ANN. tit. 5, § 4572 (2002); MD. CODE ANN., STATE GOV'T § 20-606(a) (LexisNexis 2009); MASS. ANN. LAWS ch. 151B, § 4 (LexisNexis 2008); MINN. STAT. ANN. § 363A.08(1) (West 2013); NEV. REV. STAT. ANN. § 613.330(1) (LexisNexis 2012); N.H. REV. STAT. ANN. § 354-A:7(I) (LexisNexis 2008); N.J. STAT. ANN. § 10:5-12 (West 2013); N.M. STAT. ANN. § 28-1-7(A) (LexisNexis 2013); N.Y. EXEC. LAW § 296(1)(a) (McKinney 2013); OR. REV. STAT. § 659A.030(1)(a) (2013); R.I. GEN. LAWS § 28-5-7(1)(i) (2003); VT. STAT. ANN. tit. 21, § 495(a) (2013); WASH. REV. CODE ANN. § 49.60.180 (West 2008); WIS. STAT. ANN. §§ 111.321, 111.336 (West 2002).

78. Concerning Facebook's flipping privacy settings or even prohibiting opting out without first informing users, see Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 920 (2013), Marie-Andrée Weiss, *Friends with Commercial Benefits: Social Media Users Do Not Want Their Likeness Used in Advertisements*, 16 J. INTERNET L. 1, 9 (2013), and Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165, 174 (2012).

user agreements.[79] As Richard Delgado and Jean Stefancic demonstrate in their contribution to this Symposium, without regulatory oversights, the Internet can also pose a danger to racial minorities.[80] The European Union's proposed right to erasure and its current opt-in regime—requiring "clear and comprehensive information about the purpose[s]" for which commercial vendors track their web activities—is better suited for preserving personal autonomy to one's sensitive information.[81]

The change from the U.S. self-help and opt-out approach is necessary because it provides consumers so little protection for their privacy. Topping Google and Facebook is Acxiom, which aggregates billions of records per month and offers it for resale to others.[82] Acxiom stores the personal profiles of about half a billion people worldwide, including "190 million people and 126 million households in the U.S.," in servers and storage devices that cover five acres of land, collecting and analyzing 50 trillion data transactions per year.[83] As of 2009, Acxiom estimated having about 1,500 data points "on every American."[84] Just as legitimate companies can buy this information, a witness testified at a recent Senate hearing considering whether to expand privacy regulations, thieves running scams have also exploited marketing lists that had been bought through data storage companies.[85]

The relative permanence of records kept on commercial servers, something that can be changed through an affirmative regulation, such as that discussed in Part III of this Article requiring companies to discard information after a reasonable period of time or to clearly

---

79. *See, e.g.*, Michelle Jones, *Facebook Inc (FB): Now You Can't Hide Your Profiles*, VALUEWALK (Oct. 11, 2013, 11:20 AM), http://www.valuewalk.com/2013/10/facebook-inc-fb-now-you-cant-hide-your-profiles/.

80. *See* Richard Delgado & Jean Stefanic, *Hate Speech in Cyberspace*, 49 WAKE FOREST L. REV. (forthcoming 2014) (manuscript at 10).

81. *See Data Protection in the Electronic Communications Sector*, EUROPA, http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm (last visited Mar. 2, 2014); *infra* Subpart III.A.

82. *See* R. KELLY RAINER ET AL., INTRODUCTION SYSTEMS: SUPPORTING AND TRANSFORMING BUSINESS 425 (3d ed. 2011).

83. *Acxiom Corp: The "Faceless Organization That Knows Everything About You,"* WEEK (June 20, 2012), http://theweek.com/article/index/229508/acxiom-corp-the-faceless-organization-that-knows-everything-about-you; *see also* ANDREW ROBB, BLACK DOG DAZE: PUBLIC LIFE, PRIVATE DEMONS 128 (2011) (discussing the ability of Acxiom to manage huge databases to leverage marketing data without compromising privacy concerns).

84. Stephanie Clifford, *Online Ads Follow Web Users, and Get Much More Personal*, N.Y. TIMES, July 30, 2009, at A1. Presumably "every American" referred to in the article refers to every American on whom Acxiom has data.

85. *FTC Testifies on Data Brokers Before Senate Commerce Committee on Privacy; Industry Efforts to Implement "Do Not Track" System Already Underway*, FED. TRADE COMMISSION (Mar. 16, 2011), http://www.ftc.gov/news-events/press-releases/2011/03/ftc-testifies-senate-commerce-committee-privacy-industry-efforts.

request the subjects to retain it, raises complex questions about data control and privacy. Can information from these networks be mined and augmented *ad infinitum*, without any user control or right to delete? Is the ability of private networks to amass information limitless or bounded by the personal preferences of tracked individuals? In circumstances where the interests of data services and those of private citizens conflict, can judges balance these or set categorical injunctions to limit commercial uses? When legal conflicts arise, where should they be litigated, given the seamless nature of Internet communications? How should courts deal with jurisdictional issues when litigants disseminate information that is accessible outside their own territories, states, or nations? When conflicts arise between laws of countries hosting servers and those where harms to reputation and privacy are felt, what choice of law principles should govern?

II. DATA VULNERABILITY

The extent of data gathering, selling, and free dissemination of private details, with few regulatory controls, opens many avenues for misuse. Anyone wishing to restrict access to his or her own profile has limited options because, in most circumstances, data collectors can keep, categorize, and sell captured or freely provided data without first obtaining the subject's permission for its dissemination. Even when consumers voluntarily provide their details to online stores or social networks, they have no way of controlling to whom those entities will sell the data.

Social networks are excellent fora for asserting personal control over a variety of life-fulfilling goals, allowing members to influence governance and stay in touch with friends. But individuals are not the only beneficiaries of the shift in privacy paradigms. Companies profit enormously by incentivizing disclosure of personal details. The corporate use of mined data purports to benefit the consumer, but its principal goal is the generation of revenue. Contrary to the financial interests of corporations, an individual might want to take down some revealing information that at the time of posting seemed like a good idea. Some of these messages are like tattoos that might have seemed like great ideas during a drunken binge but in hindsight would be best removed. But the current state of U.S. privacy law dealing with U.S. consumers does not require social networks or companies to delete any of the information voluntarily posted on their sites.[86] While the information remains conveniently

86. Karen Majovski, Comment, *Data Expiration, Let the User Decide: Proposed Legislation for Online User-Generated Content*, 47 U.S.F. L. REV. 807, 818–22 (2013) (discussing proposed legislation to fill this gap, and laying out the terms of such legislation).

available to find through search engines, technological architecture, proprietary interests, and trade secrets, self-help solutions are inadequate for persons seeking to purge some or all of their profiles.

Cloud servers that harvest the content of users' data for marketing have increased data vulnerability. Where a person saves information outside of his or her own computer the measure of control over personal information is further diminished. Saving documents in distant servers—administered in cloud servers owned by companies like Google, Softlayer, EarthLink, and Logicworks—is becoming increasingly popular because such sites offer users the convenience of being able to access and modify documents from any computer with Internet capabilities, rather than solely one computer with the information saved on a hard drive or the random access memory ("RAM").[87] Government officials subpoenaing documents stored on remote computing services ("RCS")[88] (cloud servers that provide additional services to simple storage, such as the cross targeted marketing and storage computer servers) do not require any court order but only that a request made to those companies coupled with the police assertion of emergent necessity requiring immediate access to prevent physical danger.[89] Because cloud servers are not simply storage locations but services that mine the content of documents as part of their services, the timeframe for warrants found in the Stored Communications Act[90] may not apply because of the distinction the law draws between electronic communications services and RCS.[91] Cloud servers fall under the latter category, which enjoys more lax standards for subpoenaing,

87. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199–200 (2010).

88. For a definition of RCS, see 18 U.S.C. § 2711(2) (2012) ("[T]he term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.").

89. PARISER, *supra* note 66, at 145–46; Joseph A. Nicholson, Note, *Plus Ultra: Third-Party Preservation in a Cloud Computing Paradigm*, 8 HASTINGS BUS. L.J. 191, 207 (2012) ("[T]he authority to access users' data for a wide variety of purposes other than mere storage or processing, such as for generating targeted advertisements, takes many cloud computing service providers outside the current SCA definition of a 'remote computing service.'"); TROUTMAN SANDERS LLP, *The Stored Communications Act and Document Subpoenas to Cloud Computing Providers*, INFO. INTERSECTION (Apr. 11, 2013), http://www.informationintersection.com/2013/04/the-stored-communications-act-and-document-subpoenas-to-cloud-computing-providers-2/ (describing how the Stored Communication Act applies to electronic communication service providers and remote computing service providers).

90. 18 U.S.C. § 2703 (establishing a warrant requirement for information that is stored for longer than 180 days).

91. Hien Timothy M. Nguyen, Note, *Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing*, 86 NOTRE DAME L. REV. 2189, 2204–08 (2011).

because they are not merely "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission"[92] but generate advertising revenues through consent from users allowing the companies to sell parts of the generated electronic content.[93] Further, during the course of litigation, a party that has used a cloud server for data storage will have less control about how to respond to production requests than if the data had been kept on its own computer or server.[94] Content placed on e-commerce websites like eBay is even easier to obtain through subpoena requests to third-party vendors without first obtaining a warrant.[95] Limits on storage times are necessary for regulating how long the cloud server can retain the data after the user demands to delete it or to altogether unsubscribe from the service.[96]

The more information that is transmitted through wireless and ethernet technologies and gathered for indefinite periods of time subject only to the business plans of data controllers, the greater the need for public oversight. The Privacy Rights Clearinghouse, a watchdog group that monitors data breaches through public records,[97] determined that between January 2005 and April 2013

---

92. 18 U.S.C. § 2510(17)(A).

93. The terms of use policy for EarthLink states, in relevant part: "EarthLink Business may use the information collected from this website . . . to provide you with more relevant offers and advertising." *Privacy Policy*, EARTHLINK BUS. (June 1, 2011), http://www.earthlinkbusiness.com/about-us/legal/privacy-policy.xea. Softlayer sets these terms:

> We may also engage Third Parties to track and analyze nonpersonally and personally identifiable website data and to serve advertisements. To do so, we may permit Third Parties to place cookies on devices of to [sic] Users of our Site, where permitted by law, and, subject to your right to opt-out through the Site 'insert link'. We use the data collected by such Third Parties to help us administer and improve the quality of the Site and to analyze Site usage. Such Third Parties may combine the information that we provide about you with other information that they have collected.

Privacy Agreement, SOFTLAYER, http://www.softlayer.com/about/legal/privacy-agreement (last visited Feb. 9, 2014).

94. Cindy Pham, Note, *E-Discovery in the Cloud Era: What's a Litigant to Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 141, 156–71 (2013).

95. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1230–34 (2004).

96. For an example of the permanency of data storage see *Google App Engine Terms of Service*, GOOGLE, https://developers.google.com/cloud/terms/deprecated-appengine-terms (last modified Apr. 1, 2013) ("Customer may select via the Service whether the Core App Engine End User Data will be stored permanently, at rest, in either the United States or the European Union, and Google will store it accordingly ('App Engine Data Location Setting'). If no selection is made, Core App Engine End User Data will be stored permanently, at rest, in the United States.").

97. *See Chronology of Data Breaches: FAQ*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breach-faq (last visited Feb. 9, 2014).

there have been at least 607.5 million data breaches online, and this figure takes into account reported events as opposed to all those that go undiscovered.[98]

Furthermore, those numbers do not even include the times Internet companies sell private records (such as financial information or search terms), many of which might be inappropriate or offensive from the subjects' perspective but lucrative from the companies'.[99] Under the current state of the law in the United States, someone would need to actively opt out of cookies or having his or her information sold to third parties, while the European Union offers consumers more control by typically requiring companies to request them to opt in.[100]

Without such limits, the data is not only helpful for marketing or litigation by private companies but also by government entities. This was brought home in 2013 with the revelation that the United States National Security Agency ("NSA") collects metadata about senders and receivers of e-mails as well as the content of the text, video, and audio.[101] The NSA also collects detailed telephone records, pursuant to the order of the Foreign Intelligence Surveillance Court of at least Verizon Business Services and likely other U.S.-based telephone companies like BellSouth and AT&T.[102] Working with companies to mine private data was not unique to President Barack Obama's administration. President George W.

---

98. *See generally* PRIVACY RIGHTS CLEARINGHOUSE, CHRONOLOGY OF DATA BREACHES (2014), *available at* https://www.privacyrights.org/sites/privacyrights.org/files/static/Chronology-of-Data-Breaches_-_Privacy-Rights-Clearinghouse.pdf.

99. Telephone Interview with Beth Givens, Dir., Privacy Rights Clearinghouse (Apr. 19, 2013).

100. Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L. REV. 7, at ¶ 10, *available at* http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf.

101. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1 ("In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records [from Yahoo and Google databanks]—including 'metadata,' which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.").

102. *See* Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html; Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, WASH. POST (June 15, 2013), http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html.

Bush's administration also engaged in warrantless domestic communications surveillance.[103] Despite private-party involvement in the controversial programs, Congress passed and Bush signed a law in 2008 that made international headlines because it retroactively immunized telecommunications companies that provided the data to carry out the surveillance.[104] Police stations around the country are also well aware of technologies' multiple utilities. Some police departments pay cell phone carriers from several hundred to more than two thousand dollars to record and turn over the whereabouts of investigation suspects' cell signals.[105] Such warrantless searches supply police with a great deal of information about alleged culprits' movements, contacts, and patterns of behavior. Without any judicial oversight it is impossible to determine how many innocent people's records police officers have reviewed or what percent of the time their hunches about the need for cell phone records have proven to be incorrect.

In rare cases, some searches of telephone records might give rise to legal challenges based on the recent holding in *United States v. Jones*.[106] In *Jones*, the police tracked a suspect who was under criminal investigation outside the geographic area permitted by a court-issued search warrant.[107] Even though the police obtained the warrant prior to proceeding with the surveillance, being beyond the judicially approved time and location was fatal to the investigation.[108] The Court held that placing of a GPS device on the person's vehicle was a warrantless trespass, violative of the Fourth Amendment.[109]

---

103. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

104. Agence France-Presse, *Bush Signs Law to Allow Wider Spy Agency Wiretaps*, EDMONTON J. (Alberta, Canada), July 11, 2008, at A13; Ramesh Thaku, *Mocking the Modern Day Messiah of U.S. Politics*, HINDU (India) (Aug. 6, 2008), http://www.thehindu.com/todays-paper/tp-opinion/mocking-the-modern-day-messiah-of-us-politics/article1309456.ece.

105. Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. TIMES (Mar. 31, 2012), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?pagewanted=all&_r=0.

106. 132 S. Ct. 945 (2012).

107. *Id.* at 948 & n.1.

108. *See id.* at 948–49 (discussing whether a warrant was necessary and implicitly assuming the warrant was invalid because the ten-day time limit had expired).

109. *Id.* at 949 (relying on trespass law to "hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'" under the Fourth Amendment); *id.* at 954 (Sotomayor, J., concurring) ("The Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection.").

By analogy, police may try to tag the GPS of a suspect's built-in cell phone device. But *Jones* has little value for anyone wishing to protect his data in the real world of cell phone surveillance: GPS units are now standard hardware in "smart phones."[110] Thus, no trespass is required for obtaining records from preinstalled devices. Without a trespass, federal courts are very unlikely to find pertinent the *Jones* limitations when it comes to the tracking of cell phone GPS records.[111] Courts consistently hold that police can subpoena suspects' phone records from third-party cellular service providers.[112] *Jones* does not prevent law enforcement agents from obtaining historical cell site records about a party's cell phone, but federal courts are divided on whether a party has any reasonable expectation of privacy to these data.[113]

---

110. *Id.* at 963 (Alito, J., concurring); United States v. Powell, 943 F. Supp. 2d 759, 767 (E.D. Mich. 2013).

111. *See* United States v. Reaves, No. 8:09CR187, 2012 WL 3137438, at *5 (D. Neb. Aug. 1, 2012) (asserting that the Supreme Court in *Jones* did not address the question of whether GPS tracking information obtained from cell phones constituted a seizure under the Fourth Amendment); United States v. Sereme, No. 2:11-CR-97-FtM-29SPC, 2012 WL 1757702, at *10 (M.D. Fla. Mar. 27, 2012) (distinguishing *Jones* because it involved search by trespass rather than the police obtaining a warrant to gain obtain cellular tracking information from cell phone carrier, and further stating that "[t]he Supreme Court has not answered the broader question presented here which is whether the Government's monitoring of an individual's movements through their cell phone for a certain period of time constitutes a 'search' within the meaning of the Fourth Amendment, and more importantly whether that 'search' requires a warrant issued upon probable cause of some other level of suspicion, such as the traditional reasonable suspicion"). On the state side, see *People v. Hall*, 926 N.Y.S.2d 514, 516 (App. Div. 2011) ("Even if a cell phone could be considered a 'tracking device' . . . to the extent that it permits the tracking of movement, the People are not thereby precluded from obtaining CSLI [cell site location information] . . . . Although [New York precedent] requires the police to obtain a warrant supported by probable cause for the installation of a global positioning system device, it does not address the matter of CSLI records.").

112. *See, e.g.*, United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011) (refusing to suppress the cell phone records obtained by the government through a subpoena because defendant did not have a reasonable expectation to privacy in that information).

113. *See* United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (holding that it does not constitute a Fourth Amendment search to locate defendant through a phone's cell-site records); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010) (holding that the third party doctrines from *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979) do not apply to information that cell phone companies retain of users' dialing history); U.S. Telecom Ass'n. v. FCC, 227 F.3d 450, 459 (D.C. Cir. 2000) (holding there is no privacy right to mobile phone tower connection); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *5, *8–14 (D. Ariz. May 8, 2013); United States v. Rigmaiden, 844 F. Supp. 2d 982, 996 n.6 (D. Ariz. 2012); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *7 (N.D. Ga. Apr. 21, 2008); *Powell*, 943 F. Supp. 2d at 771–73; Mintz v. Mark Bartelstein & Assocs., Inc., 885 F. Supp. 2d

III. LEGAL RESPONSES

The enforcement of cybersecurity laws and procedures is complicated by the transborder nature of communications media. The rapid advance in technology has created a unique set of regulatory difficulties, with the development of vast storage capacities potentially capable of tracking the day-to-day movements, shopping habits, and intellectual work of individuals through social networks, cloud servers, and e-mail systems. Without consciously and unambiguously permitting this surveillance, the subject becomes vulnerable to undesired intrusions. The U.S. consent-based norms offer consumers fewer protections than they enjoy in European countries.[114] The European Union is currently considering enacting even more rigorous standards for data retention, known as "the right to erasure."[115] Even if Europe were to adopt a regulation on the maximum time data controllers can maintain information on their servers, those companies may gravitate to the United States, where limits on retention are less likely to be successful.

People around the world are reconceptualizing privacy, posting a massive amount of information about their backgrounds, habits, friends, and families for others to view on social networks, blogs, and text messages. The laws of yesteryear are insufficient for redressing consumers' diminished autonomy. Consumers often overlook the need for regulation, judicial recourse, and remedies because of the many entrancing, commercial benefits available on new media, which make the temptation of an unregulated web seem romantic and enchanting. The Internet enhances our ability to establish and maintain associations, which is a core First Amendment right,[116] but it also forces us into associations—with businesses and natural persons—through technological architectures designed to market our personhood and make surveillance, snooping, and stalking easier. The technological advance of the Internet—just as the telephone, television, and the

---

987, 1001 (C.D. Cal. 2012) (stating that "[f]ederal courts are currently divided over whether individuals have a reasonable expectation or privacy in historic cell site information," but holding that "[f]ederal law also supports the Court's conclusion that the disclosure of telephone numbers, as well as the date, time, and duration of calls does not represent a significant intrusion of Plaintiff's privacy").

114. Determann, *supra* note 100, at ¶¶ 8, 10.

115. Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 826–27, 847 (2012).

116. Colo. Republican Fed. Campaign Comm. v. FEC, 518 U.S. 604, 615–16 (1996).

printing press before it—is not a one-way vector for social betterment.

The Internet is a godsend for ordinary people wishing to share ideas, knowledge, memories, and creativity. But the dominant players in the field are not people but service providers, social networks, and other electromagnetic service providers whose interests in profiting from personal—often highly revealing—information often conflict with consumers' desires for anonymous, risk-free browsing. Rigorous laws are necessary, and the self-help model is insufficient, for safeguarding the rights of people to maintain privacy and to decide whether corporations may track their Internet activities. The most effective regulations must not only safeguard substantive rights against commercial exploitation but also develop an effective set of procedural devices for fair trial and hearings. In this Part, I turn to how users might increase their control over digital transmissions by comparing and contrasting U.S. and EU laws, and then analyze the newest EU proposal.

Internet regulators face complex jurisdictional and substantive issues because of the Internet's cross border protocols.[117] An overly draconian domestic law can stifle the free exchange of information and might intrude into the province of foreign courts. Not providing enough legal framework, on the other hand, can result in exploitation of personal data, spread of computer viruses, and the organization of terrorism. Just as social networks, e-mails, and shared video sites can catalyze democracy and entertainment, so too can they facilitate seedy business schemes and invasions of privacy. For instance, the Internet is being used in the Middle East and North Africa both for jumpstarting democratic activists and for state espionage.[118]

European and U.S. legal approaches differ on what and whether responses are appropriate to the reduced privacy enjoyed by parties using social media. While U.S. regulations have tended to favor commercial uses of private information, the European Union has placed greater emphasis on the potential harms to personal dignity caused by the misappropriation, misdirection, or manipulation of private data.[119] Besides the personal harms—such as sexual

---

117. *See infra* Subpart III.C.

118. As President Barack Obama succinctly put it, "[T]he same GPS, satellite communications, mobile phone, and Internet technology employed by democracy activists across the Middle East and North Africa is being used against them by the regimes in Syria and Iran." Scott Wilson, *Obama Targets Rights Abuses*, WASH. POST, Apr. 23, 2012, at A5.

119. *See* Jeffrey Rosen, *Continental Divide*, LEGAL AFF., Sept.–Oct. 2004, at 49–50 ("When Europeans think about privacy, they are most concerned about personal dignity and the right to control one's public image, a right threatened primarily by the mass media, the Internet, and commercial data warehouses. By contrast, American conceptions of privacy are focused on personal liberty

harassment, job termination, and defamation—that might result from nefarious manipulation of private data, the risk of it being mined against a subject's will (and often without his or her knowledge) for wrongful purposes has led to EU negotiations about whether to promulgate a right to be forgotten and erasure, which would require a website to retain control of personal information for a reasonable period of time and then to permanently remove it from its own server and those servers under its control.[120]

The notice-and-consent regime in the United States,[121] with the broad latitude granted to data mining companies to capture an unknown quality and quantity of information about web users,[122] is significantly less protective than European standards limiting the aggregation of personal information.[123] In a recent case, the Spanish National Court ("Audiencia Nacional") held for a man who brought suit to have Google erase years-old information about his failure to pay back taxes, claiming that the precedent could set off a slippery slope of take-down orders.[124] The case has now been

---

and the right to be free from state surveillance, a right threatened primarily by government intrusions into the home.").

120. Meg Leta Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten*, 16 STAN. TECH. L. REV. 369, 371, 381–83 (2013).

121. The phrase "notice and consent" refers to whether the subjects of the information "fully understand and associate what information is being collected about them, and whether or not they're empowered to stop certain practices from taking place." *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 2 (2010) (statement of Hon. John D. Rockefeller IV, Chairman, S. Comm. on Commerce, Sci., & Transp.), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg67686/pdf/CHRG-111shrg67686.pdf.

122. FTC Commissioner Jon Leibowitz succinctly explained the degree of ignorance about the amount of data harvested from users who supposedly consent use, reuse, and resale of their data: "Today, few of us can comprehend the amount of personal data we've left open for capture on the Internet, and disclosure forms are most often written by lawyers, paid, it seems, by the syllable. The consent half of 'notice and consent' rarely reflects a consumer's conscious informed choice." *See* John Eggerton, *Leibowitz: FTC Not Interested in Regulating Behavioral Ads If Industry Can Do Job*, BROADCASTING & CABLE (May 12, 2010, 7:22 PM), http://www.broadcastingcable.com/article/452590-Leibowitz_FTC_Not_Interested_in_Regulating_Behavioral_Ads_If_Industry_Can_Do_Job.php.

123. Hannah Bloch-Wehba, Book Note, 44 N.Y.U. J. INT'L L. & POL. 692, 696 (2012) (reviewing SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFENDANT FREEDOM WITHOUT SACRIFICING LIBERTY (2011)) ("In comparing weak U.S. privacy protections to their stronger European counterparts . . . data mining and private sector data aggregation are far more constrained in Europe than in the United States, not just because of different statutory and constitutional protections, but also because data aggregation is seen to pose a concrete threat to personal privacy.").

124. *EU Judges to Hear Google 'Right to Be Forgotten' Case*, TELEGRAPH (Feb. 26, 2013, 2:45 PM), http://www.telegraph.co.uk/technology/google/9895279/EU-judges-to-hear-Google-right-to-be-forgotten-case.html.

referred to the European Court of Justice for review.[125] The results of the earlier decision pit an individual's desire to invoke European sensibility about privacy against a U.S. organization's effort to assert its right to aggregate data, even when it is unflattering to the subject.

This Part of the Article first outlines EU privacy directives and how they affect U.S. electronic service organizations with European clientele. The Safe Harbor Framework, which currently facilitates such business transactions, is likely to be expanded further if the European Union adopts right to erasure regulation into law. I next discuss the parameters, importance, and uncertainties of the proposed erasure regulation and the choice of law issues it is likely to raise.

A. European Privacy Approaches

Privacy standards vary between Europe and the United States. They differ in the treatment of free speech and the norms of civility. Europe protections against reputational harms were codified even before the advent of the Internet at the U.S. Department of Defense's Advanced Research Project Agency Network.[126] Article 10 of the 1950 European Convention on Human Rights[127] proclaims that the universal right to free expression, which includes the right to voice opinions and express ideas, is subject to the "duties and responsibilities" commensurate with such "formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society."[128] Two of the named conditions of democratic governance are the "protection of the reputation or rights of others [and] preventing the disclosure of information received in confidence."[129] Today's interactive networks and search engines present a problem of fit because much of the relevant information is not gathered clandestinely but is initially disclosed, either by the subject or her "friends," to third-party service providers. The value of privacy, nevertheless, remains the same, irrespective of whether the information was initially gathered through cookies or voluntary disclosure. The 1950 convention unequivocally asserts that "[e]veryone has the right to respect for his private and family life,

125. *Id.*

126. Tsesis, *supra* note 11, at 826–27 (discussing the early development of the Internet).

127. Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 5, *available at* http://www.echr.coe.int/Documents/Convention_ENG.pdf.

128. *Id.*

129. *Id.*

his home and his correspondence."[130] A subject does not entirely lose control of his or her data by posting them.[131]

The EU Charter of Fundamental Rights[132] adds a layer of protection, identifying the right to personal data or an intrinsic freedom.[133] The charter sets an affirmative obligation on entities to process data "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[134] What is more, anyone about whom data has been collected "has the right of access to data which has been collected concerning him or her."[135] Member states are required to develop administrative and substantive legal mechanisms to protect the processing of individuals' data.[136]

The European Directive on Data Protection of 1995[137] integrates the values of free data transfer and the need to protect the "fundamental rights and freedoms of natural persons," especially the right to privacy.[138] The directive requires members of the European Union and European states on a national level to prevent the dissemination of personal data without the knowledge of the subject, unless he or she grants unambiguous consent for specific data processing required to fulfill a contractual obligation, to abide by a legal duty, to protect the data subject's vital interests, or to perform a public function by an authorized official.[139] Controllers of data bear the primary responsibility for abiding by the terms of the directive.[140] A controller is defined to be a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[141] Data may only be collected for "specified, explicit

130. *Id.* art. 8.

131. K.U. v. Finland App., No. 2872/02, 2008 Eur. Ct. H.R. 109, 109, 111, *available at* http://hub.coe.int/c/document_library/get_file?uuid=ec21d8f2-46a9-4c6e-8184-dffd9d3e3e6b&groupId=10227.

132. Charter of Fundamental Rights of the European Union, 2010 O.J. (C 83) 389, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

133. *Id.* at 393.

134. *Id.*

135. *Id.*

136. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 51, *available at* http://eur-lex.europa.eu/en/treaties/dat/12007L/htm/C2007306EN.01004201.htm.

137. Directive 95/46/EC, of the European Parliament and of the Council, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF [hereinafter Council Directive 95/46].

138. *Id.* at 38–45.

139. *Id.* at 40.

140. *Id.* at 39.

141. *Id.* at 38.

and legitimate purposes,"[142] prohibiting techniques designed to obtain the data through the manipulation of cookies clandestinely placed on users' computing systems. To elude persons who block cookies, data miners have increasingly begun to track activities through "fingerprinting," which is a technology for analyzing computer features unique to users such as "plug-ins [sic] and software you have installed, the size of the screen, the time zone, [and] fonts."[143] Under the current regime, controllers of legally obtained data can indefinitely keep the cookies and fingerprinted information.[144]

The 2002 Electronic Communications Sector Directive[145] (the "E-Privacy Directive") further clarifies this protection by requiring anyone who places cookies to provide a "clear and precise" statement of what information was placed on the "terminal equipment."[146] The E-Privacy Directive also requires data controllers to give users meaningful opportunities to refuse those files from being mechanically stored.[147] The 2009 amendment to the 2002 E-Privacy Directive further requires third-party electronic services to give "clear and comprehensive" information about access and storage of cookies.[148] The method for informing subjects must be "user-friendly," except where the placement of a cookie is tied to an outstanding legal obligation required to achieve an electronic service subscribers or users request.[149]

Thus, European regulations require information technology companies to provide subjects with unambiguous notice of what information is being collected, why it is gathered, and who will be able to access it. A subject of data acquisition has a right to access, correct, verify, withdraw, and object to the posting and sharing of

---

142. *Id.* at 40.

143. Adam Tanner, *The Web Cookie Is Dying. Here's the Creepier Technology That Comes Next*, FORBES (June 17, 2013, 12:29 PM), http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/.

144. Ben Richmond, *How "Device Fingerprinting" Tracks You Without Cookies, Your Knowledge, or Consent*, VICE (Oct. 10, 2013, 4:55 PM), http://motherboard.vice.com/blog/device-fingerprinting-can-track-you-without-cookies-your-knowledge-or-consent.

145. Directive 2002/58, of the European Parliament and of the Council, 2002 O.J. (L 201) 37 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF [hereinafter Council Directive 2002/58].

146. *Id.* at 39.

147. *Id.* art. 5; Directive 2009/136, of the European Parliament and of the Council, 2009 O.J. (L 337) 11, 20 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF [hereinafter Council Directive 2009/136].

148. Council Directive 2009/136, *supra* note 147.

149. *Id.*

personal data.[150] These directives also restrain U.S. companies operating in Europe.[151] They are particularly helpful in protecting people from the commercial dissemination of credit records, shopping patterns, and other valuable private information.

While European regulations do not directly apply to the storage and use of personal information in the United States, the EU regime limits the transmission of data outside member states.[152] This protocol implicates the activities of multinational companies that transact in data both within and outside the European Union and that transfer data, known as "list trading," to other corporations.[153] Article 25 of the 1995 Directive on Data Protection requires member states to provide safeguards to assure that parties transferring personal data to a third country comply with any national provisions that have been adopted pursuant to other mandates of the directive.[154] However, adequacy of protection is not only judged by the formal terms of the directive; it also allows adjudicators to consider the circumstances under which the data were transferred, the type of data transfer, the reason for the transfer and the duration or conditions of storage, "the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."[155]

The U.S. method of data protection, which largely relies on self-regulation, leaves it to businesses operating in European markets to tailor terms of service agreements to meet EU standards.[156] Many data privacy standards in the United States are not mandatory but advisory, relying in large part on self-regulation. The FTC suggests that:

> (1) businesses should provide notice of what information they collect from consumers and how they use it; (2) consumers should be given choice about how information collected from

150. Council Directive 2002/58, *supra* note 145, at 45.

151. DONALD C. DOWLING, INTERNATIONAL DATA PROTECTION AND PRIVACY LAW § 24.3 (Aug. 2009), *available at* http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f 5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf.

152. *Id.*

153. *Id.*

154. Council Directive 95/46, *supra* note 137, at 45.

155. *Id.* at 46.

156. Viviane Reding, Vice-President of the European Comm'n, EU Justice Comm'r, Speech at the 2nd Annual European Data Protection and Privacy Conference: The Future of Data Protection and Transatlantic Cooperation (Dec. 6, 2011), *available at* http://europa.eu/rapid/press-release_SPEECH-11-851_en.htm ("I am worried that US 'self-regulation' will not be sufficient to achieve full interoperability between the EU and US.").

> them may be used; (3) consumers should have access to data collected about them; and (4) businesses should take reasonable steps to ensure the security of the information they collect from consumers.[157]

The FTC standards are meant to prevent deceptive data collection against the stated privacy policies of companies collecting private information against contractual use terms of their websites.[158]

In order to enable U.S. companies to engage in European markets without incurring penalties, the U.S. Department of Commerce drafted the Safe Harbor Framework ("Framework") on the transfer of personal data.[159] The Framework allows U.S. companies to voluntarily comply with the European standard for adequate privacy protection and thereby facilitates efficient international business transactions.[160] Currently, there is no limit on the time a U.S. organization can retain consumers' data, but presumably if the right to erasure should become an enforceable regulation in Europe, this would be an added Safe Harbor Framework requirement. The existing terms of operation direct organizations to provide individuals with information "in clear and conspicuous language" about the purpose for which their data are collected and how it will be used.[161] Furthermore, the organization "must offer individuals the opportunity to choose (opt out) whether their personal information is . . . to be disclosed to a third party" or used for purposes other than the reason for its original collection.[162] Sensitive information about a person's medical condition, race or ethnicity, political views, religion or philosophical leaning, membership in a trade union, or sexuality can only be disclosed to third parties with the subject's prior permission.[163] All of this information must be kept secure from "loss, misuse and unauthorized access, disclosure, alteration and destruction."[164] An organization safeguarding such data must provide opportunity to anyone wanting to access his or her own personal information in

---

157. FED. TRADE COMMN, *supra* note 8, at 7.

158. For examples of FTC cases for breaches of privacy, see *In re Microsoft Corp.*, 134 F.T.C. 709 (2002), and *In re Eli Lilly & Co.*, 133 F.T.C. 20 (2002).

159. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Jan. 24, 2014).

160. *See Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/eu/index.asp (last visited Jan. 24, 2014); *see also* Elizabeth I. Hook et al., *Transborder Law: Application of the European Union Data Privacy Law to Multinational Corporations*, 21 INT'L L. PRACTICUM 124, 126 (2008) (stating that the safe harbor requires companies "to comply with the seven Safe Harbor principles (which essentially mirror the EU Directive's seven data-quality principles and are noted below)").

161. *Safe Harbor Privacy Principles*, EXPORT.GOV (July 21, 2000), http://export.gov/safeharbor/eu/eg_main_018475.asp.

162. *Id.*

163. *Id.*

164. *Id.*

order to examine, correct, change, and even delete it.[165] The Framework is an ingenious structure of voluntary adherence that could easily lend itself to a requirement that data be eliminated after a regulatorily mandated term, when it is no longer needed for the original purpose for which it was collected. As of July 2013, 4,064 organizations were listed on the Safe Harbor Framework list, demonstrating some impact of the EU privacy directives on U.S. business.[166]

Several prominent privacy scholars recognize that persons subject to involuntary data collection have cognizable interests in the information supplied to a third party. For instance, Joel Reidenberg praises and critiques the basic framework of the EU Data Protection Directive and asserts that self-regulation is insufficient; the U.S. government should likewise exercise "information practice principles" for establishing a framework consistent with U.S. citizens' basic right of privacy.[167] Along similar lines, Lawrence Lessig argues that consumers should have a presumptive right to control information that they have revealed.[168] Lessig champions individuals' abilities to share information, but he sounds a note of caution reminiscent of the 1995 EU directive, mindful that subjects of the data maintain control over dissemination.[169] He also takes a stance in favor of persons being able to amend some records about themselves, against keeping records of information meant to be secret, and complying with storage systems allowing persons to search and prevent anyone from obtaining information without the subject's consent.[170] Another prolific privacy scholar, Paul Schwartz, recommends a "use-transfer restriction" allowing the transfer of personal data only after an individual has opted in and later also retaining the opportunity to prevent further transfers.[171]

B. The Right to Erasure

The EU's vision of democracy, with its emphasis on reputation and democracy, which appears in external agreements and member

---

165. *Id.*

166. *U.S.-EU Safe Harbor List*, EXPORT.GOV, https://safeharbor.export.gov/list.aspx (last visited Jan. 24, 2014).

167. Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 787–88 (1999).

168. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 50–51, 218 (2006).

169. *Id.* at 228.

170. *See id.* at 231.

171. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2098 (2004).

states' laws,[172] differs from the current U.S. approach, which emphasizes the right to be let alone. The European model is not fail proof against the exposure and retention of private information. Indeed, both EU and U.S. standards should be sensitive to recognize the value of transparency of information while also adhering to robust privacy requirements to balance out the autonomy rights of consumers and the public interest in limiting the availability to sensitive data.

The European Union, unlike the United States, has begun the process of formally recognizing that even data that subjects divulge voluntarily should have a maximum shelf life in controllers' servers. Even with the EU directive requirement of "unambiguous consent," there is a real risk that the subject will forget to indicate that his or her information should be kept private, forget that he or she at one point posted it and permitted third parties to market it, or lack the knowledge or time to order and then review the reams of pages of all that third-party e-companies have collected. Thus, Acxiom's recent announcement that it will soon make available upon request of consumers the vast data points it has about them is of little value because of the limitless time the company can retain the data, the lack of U.S. laws for consumers to demand corrections be made, and the lack of any mechanism for persons to demand Acxiom desist from further data mining their profiles.[173]

To meet the realities of multinational exchange involving enormous sets of data and establish privacy protections for citizens' safety and dignity, Viviane Reding, the European Commissioner for Justice, has proposed enhancing rules for securing exchanges of information while protecting people's "fundamental right to data protection."[174] Reding asserted in a 2012 speech that new regulations were needed to address advances in data technology that would prevent companies from manipulating gaps in current enforcement, which allow companies to transfer data that are kept confidential in Europe to other parts of the global market, where they can be manipulated absent stringent safeguards.[175] In October 2013, the European Parliament's Civil Liberties Committee voted for the Commission's proposal, which has now been directed for

172. See *supra* text accompanying notes 82–84 for factual details about Acxiom's data collection.

173. Adam Tanner, *Finally You'll Get to See the Secret Consumer Dossier They Have on You*, FORBES (June 25, 2013, 10:32 AM), http://www.forbes.com/sites/adamtanner/2013/06/25/finally-youll-get-to-see-the-secret-consumer-dossier-they-have-on-you/.

174. Vivian 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 3 (Jan. 22, 2012), *available at* http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm?locale=en.

175. *Id.* at 3–4.

deliberation and political negotiation between the Commission and the Council of Ministers.[176]

The proposed regulation would require businesses to inform people in "simple and clear language" how their data are being processed, including the length of time for which they plan to store the data.[177] The proposal would require companies to empower people to decide whether or not they are willing to consent to the company's intended processing of their data and to later exercise their right to withdraw permission for its processing.[178] Currently, even disclosure of an e-mail address can be linked to a panoply of personal information allowing entities unrelated to the specific transaction to formulate accurate profiles of persons by combining

---

176. Memorandum from the Eur. Comm'n on LIBE Committee Vote to Back New EU Data Protection Rules 1 (Oct. 22, 2013) [hereinafter Memo from the European Comm'n], *available at* europa.eu/rapid/press-release_MEMO-13-923_en.doc?. The current text of the proposal is:

> Article 17: Right to be forgotten and to erasure
>
> 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
>
> (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
>
> (c) the data subject objects to the processing of personal data pursuant to Article 19;
>
> (d) the processing of the data does not comply with this Regulation for other reasons.
>
> 2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

Id. at 7.

177. Reding, *supra* note 174, at 5. A recent study of EU citizens' views found that data are typically personal information disclosed through social networking sites or online shopping of whom 72% were concerned about giving away their personal data for unrelated company uses, 75% wanted to be able to delete personal information that they had previously transmitted online, and 90% of Europeans interviewed were "in favour of equal data protection rights across Europe." EU COMM'N, EUROPE THIS WEEK 27 JANUARY 2012: SAFEGUARDING FUNDAMENTAL RIGHTS—ADAPTING EU DATA PROTECTION TO THE DIGITAL AGE TO CLEAR CITIZENS' DOUBTS ABOUT THE CLOUD 2 (2012), *available at* http://europa.eu/rapid/press-release_ETW-12-2701_en.pdf.

178. Memo from the European Comm'n, *supra* note 176, at 4.

data left on various websites and public record sources.[179] This initiative builds in an enforceable right to be forgotten and erasure to deal with the Internet's almost limitless capacity for search and information retention.[180]

It would require those parties that are authorized to erase personal data to abstain from publishing and distributing it when the "data are no longer necessary in relation to the purposes for which they were collected or otherwise processed" or "the data subject withdraws consent on which the processing is based . . . or when the storage period consented to has expired, and where there is no other legal ground for processing of the data."[181] The technological feasibility of the proposal is, however, currently in doubt because of the uncertainty that media data purveyors—like Facebook, Google, or Bing—would be able to track down all the locations to which data was downloaded.[182] This hurdle could be overcome by simply requiring controllers to take down all that can be found through reasonably diligent efforts—especially all data on their own and business affiliates' servers. The solution would not be perfect but would certainly offer more privacy protections than are currently available.

If adopted, the right to be forgotten and erasure would not be absolute. For instance, it would not affect newspaper archiving or other important aspects of free speech and press. Furthermore, the

---

179. Viviane Reding, Vice President of the European Comm'n, Justice Comm'r, Speech at Intervention in the Justice Council 5 (Mar. 8, 2013), *available at* http://europa.eu/rapid/press-release_SPEECH-13-209_en.pdf ("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.").

180. Reding, *supra* note 174. Most recently the European Parliament's Legal Affairs Committee adopted the European Commission's proposals for reforming the EU's 1995 data protection rules. Memorandum from the Eur. Comm'n on EU Data Protection: European Parliament's Legal Affairs Committee Backs Uniform Data Protection Rules 1 (Mar. 19, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-233_en.pdf.

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

182. For example, Google has, in the past, lost a wide variety of data. *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/; Victoria Woollaston, *Has Gmail Lost YOUR Emails? Glitch Causes Thousands of Users to Accidentally Delete Messages and Report Others as Spam*, MAILONLINE (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.

right to erasure would not apply if there is a legal obligation to maintain and process the specific data.[183]

No similar proposal has been made in the United States, where some scholars have expressed their adamant opposition to the right to be forgotten and erasure. In order to survive First Amendment scrutiny in the United States, a unified federal regulation on the dissemination of private information will probably need to overcome heightened scrutiny analysis.[184] If Congress were to adopt a statute (rather than simply a safe harbor framework with the contractual force of law) with an opt-in provision similar to the European model, the federal policy would need to advance a substantial governmental interest.[185]

I have argued elsewhere that the primary function of government is to protect individual rights for the common good.[186] Privacy policy should meet those overlapping public-policy goals by allowing individuals to enjoy their fundamental right to privacy[187] while advancing the common good of representative democracy to facilitate the free exchange of ideas. The right to erasure would protect consumer rights and serve the public good by purging stale information with no significant public, and only corporate, value.

An individual's ability to control data he or she posts on social networks, blogs, and electronic retail sites promotes personal autonomy. Julie Cohen points out that the ability to control personal information is tied to human potentiality.[188] A person's participation in society, which involves the autonomous right to shape one's destiny, image, and sharing thoughts with others, can be undermined by the haphazard exchange of private data. The state has a substantial interest in providing the necessary privacy

---

183. HEALTH & CONSUMERS DIRECTORATE-GENERAL, EUROPEAN COMM'N, FINAL SUMMARY MINUTES, 2ND EHEALTH NETWORK MEETING 8 (Nov. 7, 2012), *available at* http://ec.europa.eu/health/ehealth/docs/ev_20121107_mi_en.pdf.

184. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2659 (2011) (holding that a statute restricting "the sale, disclosure, and use" of pharmaceutical business records is subject to heightened judicial scrutiny).

185. *See id.* at 2657, 2667–68 (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").

186. Alexander Tsesis, *Maxim Constitutionalism: Liberal Equality for the Common Good,* 91 TEX. L. REV. 1609, 1609 (2013).

187. The fundamental right of privacy is reflected in a series of landmark Supreme Court precedents. *See, e.g.*, Katz v. United States, 389 U.S. 347, 359 (1967) (holding that warrantless wiretapping of a telephone is an unreasonable search and seizure that violates a person's expectation of privacy); Griswold v. Connecticut 381 U.S. 479, 484–85 (1965) (ruling that a state prohibition on contraceptives is unconstitutional).

188. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373, 1383–84 (2000).

controls to enable individuals wanting to exercise their First Amendment right of expressing their views, some of which may be heterodox and embarrassing, without fearing job termination or personal repercussions for innocuous web postings. Unlike other authors,[189] I am not claiming that personal information can be fully characterized as property; rather, it becomes property through commercial interaction. Personal information is, instead, an intrinsic part of human dignity. Dignity, which lies at the root of privacy interests, is a commonly accepted interest in Europe[190] and one which the Supreme Court of the United States has also recognized in a variety of cases.[191]

There are nevertheless significant differences between the accepted European notion of privacy as a dignity right and United States' more libertarian ideals of free speech. The most promising means of controlling Internet speech violations have come from the

189. *See, e.g.*, Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 442 (2003); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 68–70 (1996).

190. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004) ("Continental privacy protections are, at their core, a form of protection of a right to respect and personal dignity."). The German Supreme Court, for instance, has long accepted the "basic right to informational self-determination." Steven C. Bennett et al., *Storm Clouds Gathering for Cross-Border Discovery and Data Privacy*, 13 SEDONA CONF. J. 235, 246 n.78 (2012). Two authors have called this right "the most important decision in the history of German data protection." Gerrit Hornung & Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, 25 COMPUTER L. & SECURITY REP. 84, 84–85 (2009). France has also adopted protections on privacy and dignity interests. *See* Elisabeth Logeais & Jean-Baptiste Schroeder, *The French Right to Image: An Ambiguous Concept Protecting the Human Persona*, 18 LOY. L.A. ENT. L.J. 511, 513 (1998).

191. In a case dealing with abortion rights, Justice O'Connor asserted 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). Expanding on the dignity of marriage, the Court found that the history and text of a federal statute defining marriage as only between a man and a woman "demonstrate that interference with the equal dignity of same-sex marriages, a dignity conferred by the States in the exercise of their sovereign power, was more than an incidental effect of the federal statute." United States v. Windsor, 133 S. Ct. 2675, 2693 (2013). Concurring in the *Planned Parenthood* case, Justice Stevens asserted that "[t]he woman's constitutional liberty interest also involves her freedom to decide matters of the highest privacy and the most personal nature." *Planned Parenthood*, 133 S. Ct. at 915 (Stevens, J., concurring in part and dissenting in part). In a separate case, finding unconstitutional a state statute that prohibited intimate homosexual contact, the Court explained that such a law negatively impacts affected persons' dignities. Lawrence v. Texas, 539 U.S. 558, 575 (2003). Even limits on personal mobility, including legitimate prison regulations, cannot violate "the essence of human dignity inherent in all persons." Brown v. Plata, 131 S. Ct. 1910, 1928 (2011).

FTC.[192] From my perspective, dignity interests are linked to those of personhood and autonomy, and limits on the dissemination of personal data without the consent of the subject serve to enhance consumer protections against commercial exploitation. As James Griffin, in his book *On Human Rights*, pointed out, dignity is connected to an autonomous human's ability to act effectively as a self-confident agent.[193] This is closely aligned with the German notion that personal control of one's own data is critical to self-determination and freedom.[194] These, in turn, are necessary for the normal functioning of democracy.[195] The Supreme Court's ready invocation of dignity provides a doctrinal basis for also adopting it into the field of information technology. The potential for long-term (in some cases permanent) harms to individual reputation requires sufficient protections for self-determination by empowering customers to prevent companies from using their data to further schemes unrelated to the original transaction. As things currently stand in the United States, the disclosure of most private facts posted for unrelated purposes is permitted without any prior disclosure to the subject.[196] U.S. internet service intermediaries—Google, Facebook, a blog, or other media—currently have no obligation to take down statements, photographs, or other posts uploaded by a third party, even if their content is illegal.[197] By way of contrast, in England, courts have determined that wrongful disclosure includes the republication of photographs or information

192. *See About the Federal Trade Commission*, FED. TRADE COMMISSION, http://www.ftc.gov/about-ftc (last visited Feb. 12, 2014); *see also* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 130–31 (2008).

193. JAMES GRIFFIN, ON HUMAN RIGHTS 150–52, 215, 226 (2008).

194. The German Constitutional Court explained the importance of protecting personal freedom in the technological age:

> At the heart of the constitutional order stand the worth and dignity of the person who acts through free self-determination as a member of a free society. Their protection is guaranteed by the general personality rights guaranteed in Article 2, paragraph 1 . . . of the GG, which has become particularly significant in view of modern developments and the associated new risks to human personality.

Bundesverfassungsgericht [BVerfGE] [Federal Constitutional Court] 1983 BVerfGE 65, 1 (41) (Ger.), *quoted in* 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).

195. *Id.*

196. *See* NASCIO, RES. BRIEF 3 (Sept. 2004), *available at* http://www.nascio.org/publications/documents/nascio-datamining.pdf (noting that data may be used for multiple applications).

197. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1144 n.73 (2011).

that had earlier been available to the public and are later republished by the misfeasant defendant.[198]

Several U.S. scholars, like Jane Yakowitz Bambauer, oppose enacting the proposed right to be forgotten and erasure.[199] At the same time, Bambauer acknowledges that it may be callous to forever retain electronic databases containing embarrassing, humiliating, and disreputable images, whether they are initially posted by the subjects or others.[200] Retaining a permanent record of all cyber behavior, whether by building up a dossier of search engine requests or through Facebook's refusal to expunge users' profiles, is not solely "public domain information . . . pertinent to the evaluation of a person," as Bambauer conceives it.[201] Permanent records on the Internet can become sources of the very evils—"rumor, speculation, and deniability"—that she speculates would result from a requirement that data brokers delete information after a reasonable period of time.[202] As a matter of autonomy, a person should be able to control, amend, or demand the deletion of private data that had been posted in electronic form without the subject's consent or under circumstances where the subject had not known the data were reposted or shared for significantly different reasons than the ones to which he or she consented.[203] For instance, showing info on Facebook, Google+, or MySpace about embarrassing personality traits should not become an uncensored license for employers to use in hiring and retention decisions.[204]

The effort to equate cyberspace dissemination of information with ordinary, or even newsprint, communications devalues the sea change in access to personal profiles. A state appellate court recently explained implications of the expanded availability to intimate information:

> It is true that mass communication is no longer limited to a tiny handful of commercial purveyors and that we live with

198. OBG Ltd. v. Allan, [2007] UKHL 21, [2008] 1 A.C. 1 (H.L.) [255] (appeal taken from Eng.) ("Privacy can be invaded by further publication of information or photographs already disclosed to the public."); Campbell v. MGN Ltd., [2004] UKHL 22, [2004] 2 A.C. 457 (H.L.) [12] (appeal taken from Eng.) (finding that in England wrongful disclosure of private information, which is an aspect of privacy, is actionable). *See also* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 126 (2007) (writing that English norms of confidentiality arise within the principles of dignity and "norms of relationships, trust, and reliance on promises").

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

200. *See id.*

201. *Id.*

202. *Id.* at 261.

203. *See* Calo, *supra* note 197, at 1133 (discussing objective harms from the unauthorized use of private data).

204. *See id.*

> 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, in this case complete with a photograph and other identifying features, to more than one billion Internet surfers worldwide.[205]

Nevertheless, like Bambauer, several other U.S. scholars assert that the EU's proposed right to erasure threatens free speech. For instance, Jeffrey Rosen emphatically writes that the right to erasure "represents the biggest threat to free speech on the Internet in the coming decade."[206] This is a surprisingly hyperbolic statement from such an informed expert on Internet privacy. Exponentially more threatening, dangerous, and harmful are the Russian government's deep packet searches capable of shutting down the websites of bloggers speaking out against President Vladimir Putin's government;[207] the Chinese government's exploits of Google's Gmail service for spying on its own citizens and western commercial enterprises;[208] or Belarus, Iranian, and Ethiopian use of deep packet inspection to snoop out dissent.[209] Neither is Rosen's comparison of the right to erasure to the failed effort of two Germans to erase the public record of their murder convictions analytically cogent.[210] Murder records are about matters of clear public interest in prosecuting and maintaining a record of criminal proceedings for

---

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

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

207. Thomas Grove, *Analysis: Russian Internet Attacks Stifle Political Dissent*, REUTERS (Apr. 13, 2011, 6:02 AM), http://www.reuters.com/article/2011/04/13/us-russia-internet-idUSTRE73C1P520110413; Kevin M. F. Platt, *Russia Blacklists Last Arena of Free Speech*, CGCS MEDIA WIRE (Dec. 3, 2012), http://cgcsblog.asc.upenn.edu/2012/12/03/russia-blacklists-last-arena-of-free-speech/; Andrei Soldatov & Irina Borogan, *The Kremlin's New Internet Surveillance Plan Goes Live Today, Danger Room*, WIRED (Nov. 1, 2012, 6:30 AM), http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/; Sarah Vrba, *Russians' Internet Privacy Threatened by Putin's Government*, CARE2 (June 27, 2012, 1:00 PM), http://www.care2.com/causes/russians-internet-privacy-threatened-by-putins-government.html.

208. *See* Lolita C. Baldor, *US Looking at Action Against China Cyberattacks*, NBC NEWS TECH. (Jan. 31, 2013, 7:22 PM), http://www.nbcnews.com/technology/us-looking-action-against-china-cyberattacks-1B8202819; Tom Pullar-Strecker, *Fears Surface over Chinese Cable*, STUFF.CO.NZ TECH., http://www.stuff.co.nz/technology/digital-living/5720679/Fears-surface-over-Chinese-cable (last updated Mar. 10, 2011, 8:53 AM); *Top China College Linked to Cyber-Spying Unit*, CNBC (Mar. 24, 2013, 2:04 AM), http://www.cnbc.com/id/100585097.

209. Reuters, *China's Model for Controlling the Internet Is Being Adopted Elsewhere*, ECONOMIST, Apr. 6, 2013, at 68.

210. *See* Rosen, *supra* note 206.

purposes of deterrence and, to some degree, retribution. On the other hand, private information on social media is often about intimate interactions, misleading or downright false, and derived with no due process much less criminal procedure.[211]

Rosen is correct to say that greater clarification from the European Union will be needed to guarantee that the right to be forgotten and erasure will not become a governmental bludgeon against free speech.[212] But I worry less than he about the cost of compliance to Google and Yahoo.[213] Of greater concern is the privacy of individuals whose personal information they commodify without adequate prior notice. A legal framework requiring these multibillion dollar companies to develop technologies that periodically purge records is reasonable, even though it would diminish their corporate latitude to translate users' data into advertising profiles.

Some software developments will probably be required. In the past, Yahoo has claimed that it lacks the technology needed to comply with law, only to later admit that it could quickly develop the software to abide by foreign regulations. In a well-known case, a French court found Yahoo criminally liable for allowing its auction site to be used by third parties selling Nazi paraphernalia.[214] The court ordered Yahoo to prevent advertisements of those items on its French website or to pay a daily monetary penalty for failing to comply.[215] After Yahoo brazenly claimed it was naive for the court to expect the company to filter content directed to French web surfers, the French court ordered and received an expert report that found that Yahoo could very 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."[216] Some technological hurdles will likely hinder software developers in monitoring and enforcing the EU's right to erasure. If the initiative becomes law, expert knowhow will be required to resolve the technological difficulties of enforcement, but these are not insurmountable

---

211. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1212–17 (1998) (defining some types of private electronic information).

212. *See* Rosen, *supra* note 206, at 88–90.

213. *See 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.").

214. Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181, 1184 (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).

215. *Id.* at 1184–85.

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

problems, even though they are unlikely to yield perfect fixes. The foreseeable monetary outlay for developing software should not gainsay the convincing arguments for greater consumer control of personal data.

It would be naive to believe that all personal efforts to withdraw private information from the Internet are innocent. Had the 2013 Boston Marathon bombers been able to simply delete their profiles or photos from all Internet sources before the attack,[217] their radicalization would have become invisible to investigators piecing together clues after the event. One may well protest that law enforcement requires that some information not be deleted to avoid tampering with evidence. To address this point, the EU's proposed right to erasure regulation contains a national security exception,[218] and more will need to be added to the final product in order to preserve the sort of history that can prevent against the fulfillment of conspiratorial plans and the carrying out of criminal justice. But efforts to grant consumers greater autonomy to clean up mistakes, delete old photos, and purge personal opinion posts should be treated differently, as matters personal preference of the subjects, rather than anyone and everyone who downloaded them, including ISP servers, search engines, or social network sites.

The different levels of control in the United States and Europe render it unlikely that the right to erasure will be adopted here in the near future. But the issue should at least be carefully considered because of the dignity values involved, rather than dismissed out of hand as First Amendment violation. The differences between legal systems will no doubt create distinct regulatory schemes. As we have seen, the European Union has far-reaching regulations on privacy that aim to protect information as a means of advancing people's "peace and liberty and promoting democracy on the basis of the fundamental rights."[219] In Europe, privacy is a recognized fundamental right and its enjoyment significant to the "well-being of individuals."[220] U.S. privacy law, on the other hand, is a patchwork of state-by-state and federal regulations as well as common-law torts.[221] These dissimilarities

---

217. *2011 Request for Information on Tamerlan Tsarnaev from Foreign Government*, FBI (Apr. 19, 2013), http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government.

218. *See* HEALTH & CONSUMERS DIRECTORATE-GENERAL, *supra* note 183 (noting that the proposed right to erasure does not apply when there is a legal obligation to keep and process data on a long-term basis).

219. Council Directive 95/46, *supra* note 137.

220. *Id.*

221. *See, e.g.*, Right to Financial Privacy Act of 1978, 12 U.S.C. 35 §§ 3401–3422 (2012); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012) (requiring consumer credit reporting agencies to respect consumers' privacy rights);

cannot be glossed over, but the global scale of cyberspace requires cooperation and mutual understanding.

The right to erasure regulation offers a creative solution to privacy protection on media—such as social networks, search engines, blogs, and similar websites—where the initial posts of information are often voluntary. In the social media cases, the person who posted information might nevertheless want to prevent the comprehensive compilation of all his or her data points, such as those gathered by Acxiom, especially when this gathering is done without prior permission. While a subject might be willing to share password, financial, or other personal information with particular websites for the purpose of consummating a specific transaction and even receiving advertisements from the organization, that does not imply that she is also willing to share all the proffered information with third parties to the transaction, nor for it to be retained indefinitely. Data marketing firms enable businesses to make a composite profile of each of us, available and sold by various venders on the Internet, to create a highly personalized picture that is just as private, and sometimes even more so, as the one sought in *United States Department of Justice v. Reporters Committee for Freedom of the Press*.[222] In that case, the Supreme Court recognized that compiled data, even when it is gathered from public records, can threaten privacy because multiple data points are more likely to contain mistakes and misrepresentations.[223] The mass marketing of profiles with data points gathered from public sources and across

---

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506; Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 (2012); 18 U.S.C. §§ 2510–2522; 18 U.S.C. §§ 2701–2712 (prohibiting various forms of consumer information compromise by Internet and other service providers); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710; Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 ; Health Insurance Portability and Accountability Act of 1996, Pub. Law 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 (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 (Jan. 23, 2014), http://www.ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx (listing and providing hyperlinks to seventeen states' privacy laws).

222. 489 U.S. 749, 751 (1989).

223. *Id.* at 780 (holding that requests to divulge rap sheets containing composite criminal suspect reports in response to the Freedom of Information Act are unwarranted invasions of privacy).

the Internet, which is what companies like Acxiom deliver their clients,[224] can likewise create misleading pictures.

To be clear, I am not speaking about the right to erase and alter public information but private data that are collected for specific reasons but then resold, spread, or otherwise made available on the Internet without the subject's permission. Under those circumstances, as the European Union is poised to recognize with the right to erasure, limits on the retention of data and increased control over their use by data brokers will enhance privacy.

C. Choice of Law and Clarifications on the Right to Erasure

Courts hearing breach-of-privacy and right-to-erasure claims will need to adjudicate choice of law issues because of the cross border nature of Internet communications. On occasion, First Amendment principles will be pitted against those of foreign regulations. This can occur, for instance, when a plaintiff brings proceedings in the United States to enforce a European judgment for violations of European privacy norms. For instance, data placed on cloud servers are subject to the EU regulation of informed consent to the data subject prior to their dissemination to third parties.[225] Likewise, making available subjects' geopositioning—for use in advertising and rout navigation—is subject to the European Data Directive.[226] If a U.S. court finds that the judgment violated a respondent's free-speech rights, it will deny the enforcement petition.[227] At this stage it is unknowable how U.S. courts will react to the right-to-erasure regulation. It is both feasible that they will find, as Jeffrey Rosen suggests, that the restraints on corporate prerogative are a breach of free speech,[228] or that it is a legitimate business regulation. One channel forward is to add the right to erasure to the Safe Harbor Framework, allowing U.S. firms to voluntarily follow it when interacting with European firms without giving raise to First Amendment concerns. And the current proposal, as it passed through the Civil Liberties Committee, would require any foreign company dealing with EU customers to comply with the erasure regulation.[229]

---

224. *See supra* notes 82–84 and accompanying text.

225. Council Directive 95/46, *supra* note 137, at 34.

226. *See id.* at 35.

227. *See* AARON SCHWABACH, INTERNET AND THE LAW: TECHNOLOGY, SOCIETY, AND COMPROMISES 82 (2006) (discussing state court decisions that refused to enforce foreign findings of defamation).

228. *See* Rosen, *supra* note 206.

229. *Civil Liberties MEPs Pave the Way for Stronger Data Protection in the EU*, PARLAMENTO EUROPEO (Oct. 21, 2013, 8:37 PM), http://www.europarl.europa.eu/pdfs/news/expert/infopress/20131021IPR22706_en.pdf.

EU nations recognize that choice of law considerations are subject to the constitutional restraints of member states.[230] Countries are likely to find that the balance of interests weighs on the dignity ledger of a party wanting to limit access to her information against commercial entities' desires for unlimited access to these data. The right to erasure, as one author has pointed out, is closely related to European notions of the right to "personality, encompassing several elements such as dignity, honor, and the right to private life."[231] The right to privacy is deeply rooted in the EU's Charter of Fundamental Rights.[232] In contract matters, European courts apply the law expressly named in the contract—such as might exist in a website offering services for payment while securing customers' information on the website of a business subject to the Safe Harbor Framework—or having the closest connection to the case.[233] If it were to become an enforceable regulation, the right to erasure, however, would cause Europe to deal with noncontractual obligations.

Several questions remain concerning the application of, what was then called, the right to be forgotten by European Courts that should be addressed before it becomes law. One is the timeframe for its implementation. Another issue involves choice of law principles. Typically, for noncontractual claims in the European Union, a member state's court must use "the law of the country in which the most significant element or elements of the loss or damage occur or are likely to occur" as long as the defendant could have foreseen the reasonable consequences of the publication.[234] If the same standard were to apply to the right to erasure, member states would need to adopt enforcement laws to put its terms into effect. Then there is the question of how much control an Internet carrier must exercise

---

230. *See Consolidated Versions of the Treaty on European Union*, 55 OFFICIAL J. EUR. UNION 13, 18 (2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EN:PDF (using art. 4, ¶2 of the Treaty to declare that, in general, the European Union shall respect the constitutional structures of its member states).

231. Rolf H. Weber, *The Right to Be Forgotten: More than a Pandora's Box?*, 2 J. INTELL. PROP. INFO. TECH. & ELECTRONIC COM. L. 120, 121 (2011).

232. EUROPEAN COMM'N, 2012 REPORT ON THE APPLICATION OF THE EU CHARTER OF FUNDAMENTAL RIGHTS 5, 7 (2013), *available at* http://ec.europa.eu/justice/fundamental-rights/files/charter_report_2012_en.pdf ("Europe's historical experience has led to a common understanding in Europe that privacy is an integral part of human dignity and personal freedom.").

233. Regulation 593/08, of the European Parliament and of the Council, 2008 O.J (L 77) 6 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008R0593:EN:NOT (using Articles 3 and 4 to adopt measures for cooperation in civil and commercial matters).

234. *See 2009/2170(INL) – 10/05/2012 Text Adopted by Parliament, Single Reading*, EUR. PARLIAMENT/ LEGIS. OBSERVATORY, http://www.europarl.europa.eu/oeil/popups/summary.do?id=1206289&t=e&l=en (last updated Apr. 20, 2014).

before having to delete data from a third-party's server; presumably, the supervision requirement for deletion would only apply to companies having a direct business relation with the parent corporation. Anything else would seem to be too prone to invasion of others' property interests or downright unworkable.

The content of the material to be deleted would raise the most difficult issue of all. Free speech rights must be balanced against those of privacy and dignity.[235] The European Court of Human Rights has specifically stated "[t]hat protection of private life has to be balanced against the freedom of expression."[236] The protection of speech is too important to be handled on ad hoc bases; therefore, legal guarantees will be required to assure that the right to erasure is balanced against audiences' rights to be informed.[237] Critical in this effort is retaining the interactive freedom of information technologies, which has so positively impacted global communications, while giving substantive legal value to dignity and private autonomy.

Yet another clarification requires identifying what sorts of entities will be required to comply with the right to erasure and the conditions under which it will apply to them. One example of this contextual balance already exists in Italian law, which specifically allows journalists to gather, record, and spread information necessary for news coverage without having to purge news archives.[238] Similar clarification from the European Commission is

---

235. Weber, *supra* note 231, at 122. Justice Stephen Breyer, in a book based on his Tanner Lectures, asserted similarly: "[R]evision of our laws affecting privacy requires balancing . . . in light of uncertain predictions about the technological future." BREYER, *supra* note 2, at 69.

236. Von Hannover v. Germany, 2004-VI Eur. Ct. H.R., 41, 68, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109029.

237. The right to be informed is statutorily recognized in the United States under the Freedom of Information Act. U.S. Dep't of State v. Ray, 502 U.S. 164, 177–78 (1991). In the area of commercial speech, the Supreme Court has relied on the right of audiences to know information. *See* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 754 (1996); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 756–57 (1976); Martin v. City of Struthers, 319 U.S. 141, 143 (1943). While in the United States the listener's right is implicit in the First Amendment, the European Charter of Fundamental Rights is explicit on this point: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to *receive and impart information and ideas* without interference by public authority and regardless of frontiers." Charter of Fundamental Rights of the European Union, art. 11, 2000 O.J. (C 364) 1, 11, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf (emphasis added).

238. *See* Laura Liguori & Federica De Santis, *The "Right to Be Forgotten": Privacy and Online News*, MEDIALAWS (March 18, 2011), http://www.medialaws.eu/the-"right-to-be-forgotten"-privacy-and-online-news/ (discussing Italian data protection law). *See generally* Alessandro Mantelero, *Right to Be Forgotten ed Archivi Storici Dei Giornali La Casszione Travisa il Diritto All'oblio (Right to Be*

necessary to identify what entities will be covered and the duration for which they will be allowed to retain data without asking the subjects for additional permission.

This nuanced, context-based approach may improve the likelihood that U.S. courts will enforce European judgments on electronic privacy. But the United States Supreme Court's recent statement rejecting "free-floating," "ad hoc" balancing of "social costs and benefits" against free speech concerns[239] will likely complicate congressional efforts to address privacy concerns without running afoul of First Amendment doctrine. Even though the European Model is only instructive in the United States, it provides an excellent starting point for future federal efforts. In their policy considerations, congressmen and FTC regulators should rely on "historic and traditional categories"[240] of restricted speech to prevent ad hoc politicization. Efforts to pass some version of the right to erasure in the United States might rely on congressional Commerce Clause authority to protect the dignity interests of data subject.[241] The European Union has recognized the privacy interest involved in controlling this information to be connected to human dignity,[242] and the United States Supreme Court has clearly recognized some dignity interests to be constitutional, rather than solely a sociological.[243] There is room for overlap and cooperation between in the United States and European Union to better protect data from being indiscriminately exploited by commercial vendors. In the meantime, if it becomes law, U.S. businesses dealing with European consumers will need to comply with the right to erasure or be liable for the failure.

CONCLUSION

The Internet's increased commercial importance has gone hand-in-hand with the development of sophisticated surveillance tools capable of gathering detailed profiles about web surfers. Much of the information retained by corporations can be dated,

---

Forgotten On-Line Newspaper Archives), 28 LA NUOVA GIURISPRUDENZA CIVILE COMMENTATA (CEDAM) 836 (2012), *available at* http://ssrn.com/abstract=2176835 (critiquing Italian media law in the context of the right to be forgotten).

239. United States v. Stevens, 559 U.S. 460, 470 (2010).

240. *Id.* at 468.

241. *See, e.g.*, Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 250 (1964) (approving Congress's use of the Commerce Clause to ground federal legislation protecting against deprivation of personal dignity caused by racial discrimination).

242. *See* Council Directive 95/46, *supra* note 137.

243. *See, e.g.*, Lawrence v. Texas, 539 U.S. 558, 567 (2003) (holding that the liberty protected by the Constitution allows individuals to retain their dignity by giving them the freedom to choose to engage in private, homosexual sexual conduct).

embarrassing, misleading, and defamatory. The more someone uses the Internet for personal advancement, self-fulfillment, entertainment, or education, the more private information he or she advertently and inadvertently will reveal to third parties. Data points about users can be used for developing detailed profiles about individuals to be used for commercial or political purposes. Web surfers, especially those in the United States, have little power to prevent trade in their data to third parties, whose identity they typically cannot determine.

The European model provides significantly greater protections for privacy management than the U.S. model. Government oversight is more likely to take individual interests into account than over-reliance on corporate innovations. Companies are likely to develop models to increase their ability to exploit private data for maximizing profits and growth, which is legitimate unless it infringes on data subjects' autonomy and dignity rights. Regulations against the permanent retention of data are necessary to empower consumers with greater control. This Article has sought to demonstrate how private organizations exploit technology to make far-reaching intrusions into personal lives. It has also posited the need to enhance consumers' abilities to make choices about the levels of confidentiality that third parties must exercise in the maintenance and erasure of their records. In this regard the proposed EU right to erasure would be an important positive step for consumers to retain greater control over their data.