What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers

Theodore Rostow†

Data brokers have begun to sell consumer information to individual buyers looking to track the activities of romantic interests, professional contacts, and other people of interest. The types of data available for consumer purchase seem likely to expand over the next few years. This trend invites the emergence of a new type of privacy harm, "relational control"—the influence that a person can exert on another in their social or professional networks using covertly acquired private information.

U.S. privacy laws do not protect consumers from the possibility of relational control. Moreover, few scholars have proposed reforms broad enough to address this problem. This Note surveys two frameworks which provide at least a starting point, and considers several other doctrinal shifts that might limit consumer vulnerability.

† Special thanks are owed to Amy Chua, Frank Pasquale, Joseph Falvey, Christopher Pagliarella, Paul Henderson, Mikhail Guttentag, Matthew Milano, Daniel Read, Muira McCammon, and Rebecca Crootof and the Yale Information Society Project, as well as to Inho Andrew Mun, Jenna Pavelec, Richard Frolichstein, Lauren Hobby, and the intrepid editors of the Yale Journal on Regulation.

Introduction

It has become easy to purchase data on those in one's social or professional networks. For example, $23 can buy a person's contact information and age, organizational memberships, links to social media accounts, business interests, and known associates.[1] While at first glance these data types may not appear dangerous, consumer privacy law offers remarkably few restrictions on what data can be sold to consumers. Where profit can be had, a market is likely to follow, expanding the types of data available and creating new avenues for privacy abuse.

* * *

Imagine that you are about to interview someone who has applied for a position at your company. The person does not have a perfect background, but the candidate seems like an excellent fit. During the interview, you find you share many common interests—from favorite television shows to the websites you read every morning. She shares your political sensibilities and your concerns about the future. You recommend her enthusiastically for the position, and she is hired on your recommendation. What you do not know, however, is that her personal interests and opinions were entirely feigned. She simply purchased records of your online activity—the data showing what you read and your recent purchases.

* * *

1. For example, a premium search from eVerify's people search costs $19.95 after a $2.95 charge for a five-day trial. *See, e.g.*, *Report Summary*, EVERIFY (last visited May 5, 2017), http://www.everify.com/selection.php?searchType=name&firstname=Theodore&lastname=Rostow&state=CT. This Note does not endorse this (or any other) service as an effective way to purchase consumer data.

Consumers' access to the private online activity of their peers may seem far-fetched, but it is an increasingly common problem. In India, for example, consumers can buy a person's purchase history from websites like eBay and Amazon.[2] In China, journalists have reported buying individuals' GPS data, bank balances, hotel and room information (with screenshots of the room), and internet activity for roughly 700 yuan, or $101 USD.[3] While there are no reports of these data types being available for purchase in the United States, the U.S. economy includes thousands of data brokers—companies "whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it"[4]—that sell personal data to a diverse array of actors.

In 2014, the Federal Trade Commission (FTC) published a study of the commercial practices of nine data brokers documenting the breadth of their data collection. Acxiom, one of the largest data brokers, acknowledges that it has an average of over 3000 data segments[5] on every U.S. consumer.[6] Datalogix, a broker that provides data to businesses on the spending of nearly every U.S. household, has collected data on more than one trillion dollars in consumer spending.[7] In the aftermath of the FTC report, several journalists have explored this self-regulated industry,[8] finding it expansive and profitable.[9]

2. *See* Aritra Sarkhel & Neha Alawadhi, *How Your Personal Data Sells Cheaper than Chewing Gum: How India's Fast-Growing Data Brokerage Industry Is Selling Personal Information Cheaply to Anyone Who Asks, and Why that's Dangerous*, ECONOMICTIMES (Feb. 28, 2017), http://tech.economictimes.indiatimes.com/news/internet/how-your-personal-data-sells-cheaper-than-chewing-gum/57380518 [hereinafter *India's Brokerage Industry*].

3. *See Personal Data Is up for Sale in China*, N.Y. POST (Jan. 6, 2017, 2:55 PM) [hereinafter *Personal Data*], http://nypost.com/2017/01/06/personal-data-is-up-for-sale-in-china; Rao Li Dong & Li Ling, *Southern Reporter 700 Yuan To Buy Colleagues on the Whereabouts, Including the Opportunity To Open Rooms, Internet Cafes and Other 11 Records*, SOUTHERN METROPOLIS D. (Dec. 12, 2016), http://epaper.oeeee.com/epaper/A/html/2016-12/12/content_103959.htm (original in Mandarin).

4. *FTC Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMMISSION 3 (May 2014), http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter *FTC Data Brokers*].

5. Data segments are consumer categories derived from a data (such as a consumer's marital status, vehicle purchases, and attendance at baseball games) and subsequent inferences that are based on that data. An example of a data segment is the category "Soccer Moms," which "might include all women between the ages of 21 and 45, with children, who have purchased sporting goods within the last two years[.]" *Id*. at 19. The nine brokers the FTC studied sold both actual and derived data to buyers. *Id*.

6. Data segments are consumer categories derived from a data (such as a consumer's marital status, vehicle purchases, and attendance at baseball games) and subsequent inferences that are based on that data. Examples of data segments include "Soccer Moms," which, for example, might include all women between the ages of 21 and 45, with children, who have purchased sporting goods within the last two years." *Id*. at 8.

7. *Id*. at 9.

8. *See, e.g.*, Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016), http://www.newsweek.com/secretive-world-selling-data-about-you-464789; Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Mar. 9, 2014), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information; *see also FTC Data*

While most brokers generate profits by selling data to commercial entities, many have begun to generate significant revenue by also selling data to individual consumers.[10] Of the nine firms the FTC studied in 2014, three offered these services and together generated more than $52 million in annual revenue. The data products they sold were designed primarily for individual consumers, who use the "products for such purposes as tracking the activities of executives and competitors, finding old friends, researching a potential love interest or neighbor, networking, or locating court records."[11]

While a growing number of privacy scholars have written on the data broker industry,[12] this Note is the first to consider the implications of an unregulated data market that allows individual consumers to purchase information about others without their knowledge or consent.

A. Considering a New Privacy Harm

Over the past two decades, privacy law and scholarship have been pre-occupied by a central question: what is the harm in a privacy violation?[13] Courts require plaintiffs to show a concrete, particular harm before they will recognize a privacy violation.[14] This legal requirement has led privacy scholars

Brokers, *supra* note 4, at 17 (describing self-imposed contractual protections that some brokers unilaterally adopt).

9. *See, e.g.*, Emily Steel, *Financial Worth of Data Comes in at Under a Penny a Piece*, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/intl/cms/s/0/3cb056c6-d343-11e2-b3ff-00144feab7de.html (describing how the "multibillion-dollar data broker industry profits on the trade of thousands of details about individuals . . . [, which] often are sold for a fraction of a penny apiece.").

10. *FTC Data Brokers*, *supra* note 4, at 34.

11. *Id.*

12. *See, e.g.*, Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 788 (2016); Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots"*, 2014 MICH. ST. L. REV. 1411; David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 498 (2016); Ashley Kuempel, Comment, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207 (2016).

13. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 (2011). The focus on digital privacy's harm has evolved, at least partially, in response to early critiques that digital privacy interests were economically inefficient or could not be rooted in viable constitutional claims. *See, e.g.*, Robert H. Bork, *The Right to Privacy: The Construction of a Constitutional Time Bomb*, *in* PRINCIPLES OF CONSTITUTIONAL INTERPRETATION 311 (1990); Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981).

14. *See, e.g.*, Spokeo v. Robbins, 136 S. Ct. 1540 (2016) (vacating and remanding the 9th Circuit for "elid[ing] independent 'concreteness' requirement" in its injury-in-fact analysis); *see also In re* Google, Inc. Privacy Policy Litigation, Case No. C-12-01382-PSG, 2013 WL 6248499, at *3 (N.D. Cal. Dec. 3, 2013) (dismissing plaintiffs' complaints against Google for compiling personally identifiable information across different Google services, because plaintiffs failed to meet Article III standing requirements by showing "(1) [plaintiff] has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision"); *see also* Calo, *supra* note 13, at 1132 ("A privacy harm must be 'cognizable', 'actual,' 'specific,' 'material,' 'fundamental,' or 'special' before a court will consider awarding compensation.").

to devote considerable energy to identifying (or dismissing)[15] the harms that a violation of privacy can cause.[16]

Scholars have mapped privacy harms that flow from the collection,[17] aggregation,[18] use,[19] and dissemination[20] of digital information.[21] These harms

15. *See, e.g.*, STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010); AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999); Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 251 ("Privacy is the terrorist's best friend . . . .").

16. For example, Daniel Solove sought to map all privacy harms that can be connected to digital activity. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482 (2006) (providing a "comprehensive and concrete" description of harms associated with information collection, processing, dissemination, and intrusion). Recent scholarship has built on his efforts, especially with respect to the discriminatory implications of "big data." *See e.g.*, Schmitz, *supra* note 12; *see also* Kuempel, *supra* note 12, at 207 (underscoring the discriminatory implications of data commoditization). In a 2015 article surveying the history of privacy regulation in the United States, Maureen Ohlhausen and Alexander Okuliar conclude that inquiries into the type and scope of harm, along with the possibility of remedy, remain the best way to determine how legally to respond to a privacy concern. *See* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* The Right *[Approach]* to Privacy, 80 ANTITRUST L.J. 121, 153-55 (2015). Nevertheless, some privacy scholars consider the harms related to privacy violations to be thoroughly mapped, and some scholars have looked to move away from a focus on privacy harm. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1164-65 (2015) (providing examples of scholars moving away from a focus on privacy harm).

17. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000); Paul M. Shwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656 (1999); Solove, *supra* note 16, at 493 ("Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behavior . . . . lead[ing] to self-censorship and inhibition.").

18. *See, e.g.*, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, EXEC. OFFICE PRESIDENT (May 2016), http://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf; DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1-10 (2004) (describing the tailored "digital dossiers" that are collected and how this can be harmful in the context of government access to information); Raymond Daniel Moss, Note, *Civil Rights Enforcement in the Era of Big Data: Algorithmic Discrimination and the Computer Fraud and Abuse Act*, 48 COLUM. HUM. RTS. L. REV. (forthcoming 2017).

19. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Jonathan Zittrain, Response, *Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy*, 127 HARV. L. REV. F. 335, 335-36 (2014), http://harvardlawreview.org/2014/06/engineering-an-election; Bruce Schneier, *Why Uber's 'God View' Is Creepy*, CNN (Dec. 4, 2014, 8:03 AM), http://www.cnn.com/2014/12/04/opinion/schneier-uber-privacy-issue; Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

20. In recent well-publicized instances, both commercial entities and hackers have used the threat of dissemination to try to extort concessions from individuals. *See* Balkin, *supra* note 19, at 1187-94 (describing Uber's efforts to "dig up dirt" on a critical Buzzfeed reporter); Laurie Segall, *Ashley Madison Users Now Facing Extortion*, CNNMONEY (Aug. 21, 2015, 7:00 PM), http://money.cnn.com/2015/08/21/technology/ashley-madison-users-extorted.

21. *See, e.g.*, Solove, *supra* note 16, at 492-94 (providing a "comprehensive and concrete" description of harms associated with information collection, processing, dissemination, and intrusion); *see also* THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.

range[22] from less tangible—including ill ease or anxiety at the prospect of being constantly monitored[23] (which can also lead to self-censorship[24]), consumer manipulation by companies,[25] and voter manipulation by campaigns[26]—to more tangible harms, such as blackmail[27] and stalking.[28] Identified harms also manifest in social sorting and discrimination,[29] an increased vulnerability to cyber attacks,[30] and identity theft.[31]

Scholarship that has analyzed the privacy implications of the data broker industry discuss harms parallel to those that Daniel Solove and others have previously identified. David Vladeck's analysis of the broker industry highlights three privacy harms—identity theft (the most urgent), data breaches, and the unrestrained collection of sensitive, personal data.[32] Rebecca Lipman's work underscores both how data brokers provide capacity for third parties to deliver targeted advertising,[33] as well as how these datasets can facilitate harmful social sorting.[34] Amy Schmitz argues that data sales can encourage

22. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131 (2011) (describing the boundaries of "objective" harms—involving financial, dignitary, or other tangible loss—and "subjective" harms—involving psychological ill-ease or distress).

23. *See, e.g.*, Solove, *supra* note 16, at 493 ("[D]irect awareness of surveillance [can] make a person feel extremely uncomfortable . . . ."); *see also* Tatiana Siegel, *Sony Hack Fallout: Executives Now "Afraid" To Send Emails*, HOLLYWOOD REP. (Dec. 17, 2014), http://www.hollywoodreporter.com/news/sony-hack-fallout-executives-afraid-758506.

24. *See, e.g.*, Cohen, *supra* note 17, at 1426 ("[P]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."); Shwartz, *supra* note 17, at 1656 (arguing that the internet's constant surveillance of the "naked thought's digital expression short-circuits the individual's own process of decisionmaking").

25. *See, e.g.*, sources cited in *supra* note 12; Andrew Hasty, Note, *Treating Consumer Data Like Oil: How Re-framing Digital Interactions Might Bolster the Federal Trade Commission's New Privacy Framework*, 67 FED. COMM. L.J. 293, 300 (2015).

26. *See, e.g.*, Bruce Schneier, *Candidates Won't Hesitate To Use Manipulative Advertising To Score Votes*, GUARDIAN (Feb. 4, 2016, 6:45 AM), http://www.theguardian.com/commentisfree/2016/feb/04/presidential-election-voter-data-manipulative-advertising-privacy.

27. *See, e.g.,* Balkin, *supra* note 19, at 1187-94 (describing Uber's attempt to find embarrassing information on a reporter to dissuade her from continuing to write negative stories about the company); Segall, *supra* note 20.

28. *See, e.g.*, Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003) (describing a New Hampshire resident's purchase of an acquaintance's personal information from an information broker in order to stalk and ultimately murder her).

29. *See, e.g.*, Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2091-93 (2015) (describing the privacy interest in avoiding social sorting, which involves "obtain[ing] personal and group data in order to classify people and populations according to varying criteria" and discrimination); Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735 (2015).

30. Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 454-59 (2014) (describing how the prominence of data sale and bulk data brokers exacerbates data vulnerability).

31. Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1229 (2003).

32. Vladeck, *supra* note 12, at 501-12.

33. *Cf.* Slade Bond, *Doctor Zuckerberg: Or, How I Learned To Stop Worrying and Love Behavioral Advertising*, 20 KAN. J.L. & PUB. POL'Y 129 (2010).

34. Lipman, *supra* note 12, at 781-82.

discrimination and reinforce preexisting power imbalances through the secret scoring and segmenting of consumers' economic value.[35] However, these important concerns do not contemplate distinct, new harms that may stem from the sale of digital information.

This Note adds to the scholarship on data sales by arguing that the creation of a market for individuals to buy data on their peers enables a new privacy harm: "relational control." Relational control occurs when individuals acquire the private data of those in their social or professional networks. When data brokers sell consumer data to individuals, they allow buyers to learn about the behavior and motivations of those whose data they purchase. These insights allow the buyers to influence the decisions of those around them, leading to potential harms unrecognized by privacy scholarship to date.

This Note proceeds in six parts. Part I surveys the data broker industry and the market for data that is sold to individuals. Part II reviews existing U.S. commercial privacy law and explores how the law fails to protect consumers from or provide remedies for most relational control harms. Part III elaborates on the theoretical premises of the relational control harm and outlines why this threat is likely to grow.

Part IV assesses the interventions that scholars and technologists have offered to combat commercial privacy threats and explains why these reforms fail to remedy consumer exposure to relational control. Part V explains why two recent frameworks—Paul Ohm's "sensitive data" theory and Jack Balkin's "information fiduciaries" theory—offer possible paths to reduce the likelihood of relational control, although neither is designed to prevent a relational control harm.

Finally, Part VI proposes a number of doctrinal shifts in existing privacy law that may reduce consumer exposure to relational control. Congress and state legislatures could also move to protect certain types of information as sensitive and impose heightened diligence and consent standards (or an outright ban) on transactions involving these types of information. Common law courts could also expand tort law to allow consumers harmed by relational control to sue where information was wrongly used or sold. However, none of these proposals is a panacea, and, further, each could prove economically disruptive. Though there are a number of ways to reduce consumer exposure, the problem of relational control is not easily solved.

I. The Data Broker Industry and the Market for Buying People's Data

This Part introduces what is currently known about the data broker industry and the sale of consumer information to individuals.

35. Schmitz, *supra* note 12.

A. An Expansive U.S. Broker Industry

The data broker industry in the United States has expanded considerably over the past few years. A 2016 *Newsweek* report estimates that the industry includes between 2500 and 4000 data brokers.[36] Unlike large companies like Google and Facebook, data brokers try to avoid name recognition[37] while collecting data on American consumers.[38]

Brokers collect information from a combination of public records, publicly available information, and non-public, proprietary sources.[39] Major public sources of data are federal and state governments, which provide consumer information relating to recreational and professional licenses; bankruptcies; driving histories; voter registration; mortgages; and birth, marriage, divorce, and death records.[40] Data brokers also scrape publicly available data from social networking sites and blogs, and buy and sell private data from digital services.[41] Of the nine data brokers the FTC surveyed in 2014, eight bought data from commercial entities, including purchase information (such as dates of transactions, dollar amounts spent, and types of card used), and aggregated transactional data from financial services companies.[42] At least one of the nine brokers purchased consumers' web browsing activities from online advertising networks.[43] As many commentators note, there is no legal regime that prevents brokers and other companies from sharing data with individuals and companies.[44] A wide array of entities—from political campaigns[45] to antivirus companies[46]—buy and sell data with brokers.[47]

36. Boutin, *supra* note 8.

37. Kroft, *supra* note 8 ("What most of you don't know, or are just beginning to realize, is that a much greater and more immediate threat to your privacy is coming from thousands of companies you've probably never heard of, in the name of commerce.").

38. Vladeck, *supra* note 12, at 498 ("Make no mistake, there is little question that the major data brokers know more about each of us than, say, for example, the National Security Agency, the Internal Revenue Service, the Social Security Administration, or any other government institution.").

39. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 3-4 (2013) [hereinafter *GAO Information Resellers*].

40. *See FTC Data Brokers*, *supra* note 4, at 11-13.

41. *See id*. at 13-14.

42. *See id*. at 13-14.

43. *See id*. at 14.

44. *See, e.g*., Boutin, *supra* note 8 ("As shady as it might sound, the entire industry is completely legal.").

45. *See, e.g*., Neal Ungerleider, *Yes, Political Campaigns Follow Your Browser History*, FASTCOMPANY (Nov. 5, 2013, 9:30 AM), http://www.fastcompany.com/3021092/yes-political-campaigns-follow-your-browser-history ("There are few laws preventing marketing firms working on election campaigns (or, for that matter, selling laundry) . . . .").

46. *See, e.g*., James Temperton, *AVG Can Sell Your Browsing and Search History to Advertisers*, WIRED (Sept. 18, 2015), http://www.wired.co.uk/article/avg-privacy-policy-browser-search-data ("While AVG has not utilised data models to date, we may, in the future, provided that it is anonymous, non-personal data, and we are confident that our users have sufficient information and control to make an informed choice.").

B. Data Sales to Individual Consumers

Selling big data is lucrative. The nine brokers surveyed generated a combined $426 million in annual revenue. In general, this revenue stemmed from three business lines: marketing, risk mitigation, and "people search."[48] Most relevant to this Note's inquiry is people search, as the services that comprise people search are "often intended for use by individuals."[49] The FTC noted that "users utilize people search products for such purposes as *tracking the activities of executives and competitors*, finding old friends, *researching a potential love interest or neighbor*, *networking*, or locating court records."[50] Three of the nine brokers offered people search products and generated a combined $52.69 million in annual revenue.[51]

The number of brokers offering people search services in the United States remains unknown. In 2014, reporter Julia Angwin documented her attempts to opt out from over 200 data brokers, including sixty-four that specialized in people search services.[52] In 2015, columnist Cynthia Alice Andrews compiled a directory of the websites and privacy policies of 257 people search services.[53]

With few exceptions, little is known about the types of information that these brokers sell to consumers. Some well-known brokers like Spokeo only sell information derived from public sources. However, there are hundreds of brokers that offer people search services in the United States, and it is unlikely that each refrains from selling non-public information. A 2013 GAO report on the data broker industry notes, without naming specific companies, that U.S. brokers offer people search services that incorporate data from "proprietary sources" in addition to information that consumers make publicly available or

47. *See e.g.*, Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, PROPUBLICA (June 11, 2011, 11:45 AM), http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you ("[T]he credit reporting giant Experian performs a 'double-blind' match between Microsoft's data and campaigns' data. Yahoo uses another massive data company, Acxiom. Both Experian and Acxiom also offer similar matching for commercial clients who want to find previous customers online."). The use of double-blind or other anonymization features is particularly susceptible to de-anonymization, even by a "regular" consumer. *See infra* Part III.

48. *See FTC Data Brokers*, *supra* note 4, at 23.

49. *Id*. at 34.

50. *Id*. (emphasis added).

51. *Id*. Some brokers offer limited versions of their people search products to consumers for free A spokesperson for the people search broker Whitepages claimed that its free search service received 55 million unique visitors every month. *See* Kaveh Waddell, *How FamilyTreeNow Makes Stalking Easy*, ATLANTIC (Jan. 17, 2017), http://www.theatlantic.com/technology/archive/2017/01/the-webs-many-search-engines-for-your-personal-information/513323 ("With that volume of visitors, we do our best to make sure we're only offering up landline telephone numbers and addresses" to users who don't pay for [its $30 a month "Premium" service]. . . .")

52. *See* Julie Angwin, *Privacy Tools: Opting Out from Data Brokers* (Jan. 30, 2014), http://juliaangwin.com/privacy-tools-opting-out-from-data-brokers.

53. *See* Cynthia Alice Andrews, *Breaking It Down: The Data On Data Brokers*, FLIP MEDIA (Feb. 09, 2015), http://flipthemedia.com/2015/02/breaking-data-data-brokers.

exists in public records.[54] And, as noted, brokers in other countries have begun to sell individuals consumer data that originates from, among others, proprietary sources in the United States like eBay and Amazon.[55]

II. Gaps in U.S. Commercial Privacy Law

U.S. commercial privacy protections are derived from distinct, intersecting authorities—including federal and state statutory law, tort law, agency regulations, promulgated industry best practices, and private contractual agreements. This Part surveys how these authorities provide few checks on the sale of consumer data.

A. Statutory Privacy Protections in the Commercial Sphere

The United States has adopted a patchwork, sectoral approach to federal privacy law in the commercial sphere.[56] The Telecommunications Act bars ISPs from using, disclosing, or permitting access to "individually identifiable customer proprietary network information" for purposes outside of the provision of the telecommunications services from which the information is derived.[57]

Beyond ISPs, the Fair Credit Reporting Act (FCRA) imposes an array of obligations on consumer reporting agencies and offers protections for personal credit information.[58] For example, the FCRA grants individuals the right to request a copy of their credit report, limits the purposes for which a credit report can be used,[59] and obligates agencies to correct errant information.[60]

The Health Information Portability and Accountability Act (HIPAA) governs how doctors and medical services must protect the data of their patients.[61] HIPAA mandated that the Secretary of Health and Human Services (HHS) promulgate rules for certain health information controlled by providers,

54. *See GAO Information Resellers*, *supra* note 39, at 3-4.

55. *See* sources cited in *supra* notes 2-3.

56. *See, e.g.*, DANIEL J. SOLOVE & PAUL H. SCHWARTZ, INFORMATION PRIVACY LAW 790-98 (5th ed. 2015) (describing the various privacy laws that regulate distinct sectors of U.S. industry); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of The Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1217 (2013).

57. 47 U.S.C. § 222 (2012). This prohibition exists notwithstanding the recent law that set aside the FCC's October 2016 rule, which would have prevented ISPs from selling a consumer's data with out their opt-in permission. *See* Alex Johnson, *Trump Signs Measure To Let ISPs Sell Your Data Without Consent*, NBC News (Apr. 3, 2017), http://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316 (referring to S.J. Res. 34, 115th Cong. (2017)).

58. *See* Fair Credit Reporting Act, Pub. L. No. 91-508, § 601, 84 Stat. 1114, 1128 (1970) (codified as amended in scattered sections of 15 U.S.C.).

59. *See* 15 U.S.C. § 1681b (2012).

60. *See, e.g.*, *FCRA Summary of Rights*, EQUIFAX (last visited Feb. 18, 2017), http://www.equifax.com/privacy/fcra.

61. *See* Health Information Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29 & 42 U.S.C.).

health care plans, and clearinghouses.[62] The HHS privacy rule aims to safeguard all "protected health information"—individually identifiable information, including demographic data, and information relating to a patient's medical background and care—that these entities hold. The privacy rule establishes a set of national standards for protecting patient information, including setting standards for sufficiently de-identified data.[63]

The Gramm-Leach-Bliley Act (GBLA) and the Family Educational Rights and Privacy Act (FERPA) regulate the financial and education services, respectively. FERPA bars disclosure of students' educational records.[64] The GLBA requires that covered financial services entities give notice of their privacy practices, secure customer records, and provide a right for consumers to opt out of data sharing with third parties.[65]

A particularly important piece of legislation to this Note's inquiry is the Stored Communications Act (SCA),[66] passed by Congress as part of the Electronic Communications Privacy Act of 1986 (ECPA).[67] The SCA prohibits electronic communications providers from disclosing digital communications to nongovernmental entities without the consent of the message's originator or recipient.[68]

However, the adequacy of existing federal statutory protections should not be overstated and many scholars have questioned their fundamental efficacy.[69] A common critique is that these statutes protect particular channels of data flow, rather than certain data types or data that may be relevant to certain recognized private interests.[70] For example, Rebecca Lipman describes how HIPAA does not apply to health data that is generated by FitBits, Google Searches, Apple Watches, or other devices that comprise the Internet of Things.[71] Similarly, FERPA does not impose rules on the data that commercial studying applications collect, which allows companies to make "consequential

62. *See* 42 U.S.C. § 1320(d)(2) (2012).

63. *See* HIPAA Privacy Rule, 45 C.F.R. pt. 164.514(b)-(c) (2002); *infra* Part III.

64. *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012).

65. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.); Chris Hoofnagle, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, B-1 The United States of America*, EUR. COMMISSION: DIRECTORATE-GENERAL JUST., FREEDOM & SECURITY 3 (May 2010), http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf.

66. 18 U.S.C. §§ 2701-12 (2012).

67. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

68. *See* 18 U.S.C. § 2702 (2012).

69. *See, e.g.*, Tene, *supra* note 56, at 1217 ("At best, the current framework strains to keep up with new developments; at worst, it has become irrelevant.").

70. *See, e.g.*, Ohm, *supra* note 16, at 1191.

71. Lipman, *supra* note 12, at 788; *id.* at 803 (describing the growing number of devices and household appliances that are connected to the internet for the purposes of convenient remote control, energy efficiency, and data tracking).

inferences" about "a child's intelligence or interests."[72] Paul Ohm notes how the GLBA only applies to a narrow subset of entities that are defined by the statute as "financial institution[s]."[73] Congress has also relaxed certain restrictions that would otherwise protect certain types of digital data. Ohm notes how the Video Privacy Protection Act (VPPA), passed by Congress after a reporter publicized Judge Robert Bork's video rental records during his Supreme Court confirmation hearings, was amended so as not to apply to online video streaming after Netflix waged a lengthy campaign to relax protections.[74]

As a general rule, statutes do not prevent brokers from buying and selling an enormous amount of information, digitally produced by consumers, relating to their health and physiology, cognitive abilities, interests, purchases, wealth, compulsions, and social networks. Two noteworthy exceptions to this trend are the (flawed[75]) SCA and (far stronger) Children's Online Privacy Act (COPPA).[76] Despite describing an outdated technical reality, courts have interpreted the SCA to protect certain digital communications that many applications cannot sell to third parties.[77] The SCA, however, does not extend to social media posting or comments, and its language—passed in 1986 as part of the Electronic Communications Privacy Act—no longer coheres in today's technological environment.[78] In contrast, COPPA provides robust protection of the privacy of minors. Ohm notes how COPPA "applies broadly to any 'operators of websites and online services,' without further limitation,"[79] and the FTC has made clear that this definition expands as technology changes to cover mobile apps, browser plug ins, and third-party networks.[80] These narrow exceptions notwithstanding, Congress has passed no statute that imposes checks on, or regulation of, data broker activity.

State legislation similarly provides few checks on broker activity. California has moved to expand privacy protections more than any other state, but its regulations generally do not reach data brokers. California has passed legislation that (1) expands the SCA to prohibit employers from looking at the

72. *Id*.

73. Ohm, *supra* note 16, at 1190 n.362.

74. *Id*. at 1140.

75. *See* 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 (2004); *see also* Matter of Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197 (2d Cir. 2016) (Lynch, J., concurring) (pointing to Kerr's critiques from more than twelve years prior as evidence of pressing need for Congress to revisit the statute).

76. *See* Child Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728, 15 U.S.C. §§ 6501-06.

77. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (2010).

78. *See* 18 U.S.C. § 2702 (2012) (distinguishing entities that provide "electronic communications services" (ECS) and "remote communications services" (RCS)); Kerr, *supra* note 75; *infra* Part VI.

79. Ohm, *supra* note 16, at 1192 (quoting COPPA).

80. 16 C.F.R. pt. 312.

private social networks of employees and prospective employees (which does not apply to data brokers),[81] (2) requires businesses that collect personally identifiable information to prominently display their privacy policy (which applies to data brokers)[82] and (3) requires companies to disclose what information they share with other companies for marketing purposes (which does not).[83] Additionally, scholars note that, outside of California, other state legislatures thus far avoided imposing new regulations on the data broker industry.[84]

B. Judicial Limitations on Privacy Protection

Absent statutes, courts provide little protection from possible abuses that may arise from the commoditization of data. For the past fifty years, courts have recognized four privacy torts: intrusion, public disclosure of private facts, false light, and appropriation.[85] Of the four, relational control most directly implicates the intrusion tort, as a purchaser attempts to gain access to private information by purchasing another's data. The Second Restatement of Torts defines the intrusion tort as: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be *highly offensive* to a reasonable person."[86]

In addition to showing that a data transaction constitutes an intrusion upon one's seclusion (or satisfies a statutory hook, like the FCRA), a plaintiff must also demonstrate that the harm satisfies Article III standing requirements. To show standing, a plaintiff must demonstrate (1) an injury-in-fact that is concrete

81. California Social Media Privacy Act of 2012, CAL. LAB. CODE § 980 (West 2012).

82. CAL. CIV. CODE § 1798.83(b) (2006).

83. CAL. CIV. CODE § 1798.83(a)(1), (e)(6)(A) (2006); *see* Lipman, *supra* note 12, at 794.

84. *See, e.g.*, Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 810 (2016) (highlighting the efforts of former FTC Commissioner Julie Brill to press state attorneys general to investigate data brokers under state Unfair and Deceptive Acts and Practices statutes). Historically, state legislation has focused on data security rather than privacy. *See, e.g.*, The Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255 (2005) (describing a number of state data security laws and highlighting California's oft-discussed and widely praised Security Breach Information Act); Ohm, *supra* note 16, at 1127 n.3. However, this trend may be shifting, as state legislatures, attorneys general, and privacy advocates look to use state power to protect consumer privacy. *See, e.g.*, Erin Golden, *Minnesota Legislature Pushes Back on Internet Privacy*, STAR TRIBUNE (Mar. 30, 2017), http://www.startribune.com/minnesota-legislature-pushes-back-on-internet-privacy/417670943; Press Release, Maura Healey, *Attorney General of Massachusetts, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities* (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

85. *See, e.g.*, William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

86. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977) (emphasis added).

and particularized,[87] (2) "fairly traceable to the challenged conduct of the defendant, and (3) likely to be redressed by a favorable judicial decision."[88] These twin standing and tort requirements have led courts to reject most privacy claims that challenge the sale of information.

In *Shibley v. Time, Inc.*, an Ohio court dismissed a plaintiff's suit against magazine publishers that sold subscription requests to direct mail advertisers.[89] The court held that although the purchasers of the lists could learn about the plaintiff's lifestyle, the sale of lists would not "cause mental suffering, shame or humiliation to a person of ordinary sensibilities."[90] Similarly, in *Dwyer v. American Express Co*., an Illinois appellate court rejected a plaintiff's privacy suit that objected to American Express's sale of consumer profiles that were derived from their spending habits.[91] The *Dwyer* court similarly held that American Express's sale of consumer profiles did not meet the standards for one of the four types of privacy tort.

On one occasion a New Hampshire court, faced with a particularly grisly murder, left the door ajar that a data broker might be liable for negligence, where criminal activity could have been predicted. In *Remsburg v. Docusearch, Inc.*,[92] a New Hampshire resident purchased an acquaintance's personal information from an information broker in order to stalk and ultimately murder her. Due to the particular targeted nature of the New Hampshire resident's inquiries,[93] the court found that an early data broker might be liable for negligence if the buyer's manifested activity suggested foreseeable criminal misconduct against the target of his data acquisition. However, the court noted that the possibility of this narrow exception runs against the general presumption that "a private citizen has no general duty to protect others from the criminal attacks of third parties."[94] As a general rule, courts have not restricted the sale of data under either tort or statutory law.

C. Agency Regulation of Data Transactions

In contrast to the statutory and judicial remedies, federal agencies have proved more responsive to digital privacy concerns. Of recent significance is the (now repealed)[95] 2016 action by the Federal Communications Commission

87. *See* sources cited in *supra* note 14 and accompanying text (vacating the 9th Circuit ruling and remanding because the claim failed to satisfy standing requirements).

88. Spokeo v. Robbins, 136 S. Ct. 1540, 1547 (2016).

89. Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio App. 1975).

90. *Id*. at 339.

91. Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. 1995).

92. 816 A.2d 1001 (2003).

93. The resident sought at different times the date of birth, social security number, and home address, for one person, and the resident paid over $200 for the information. *See id*. at 1006-07.

94. *Id*. at 1006-07; *cf*. SEINFELD, *The Finale* (television broadcast May 14, 1998) ("You don't have to help *anybody*! That's what this country's all about!").

95. *See supra* note 57.

(FCC) to require ISPs to disclose the types of information they collect and gain consumer consent to sell their data.[96] Had it gone into effect, the privacy rule would have required ISPs to disclose the types of information that they collect, the purposes for which the data are used, and what information they share.[97]

Beyond the purview of ISP regulation,[98] the FTC has been the leading advocate for consumer privacy, issuing over 170 privacy complaints against companies for privacy violations.[99] The FTC derives its authority from Section 5 of the Federal Trade Commission Act to prohibit "unfair or deceptive acts or practices."[100] Under this authority, the FTC targets an array of commercial privacy practices. For example, the FTC entered into a consent decree with Snapchat after the agency learned that the company stored messages on its servers, despite its claims that those messages would disappear.[101] As part of the consent decree, Snapchat agreed to submit to twenty years of monitoring to ensure it did not deceive customers.[102] The FTC has entered into similar consent decrees with Facebook, when in its early days the company did not adhere to its own privacy policies,[103] as well as other apps whose privacy policies are deceptive (as opposed to merely vague and lawyerly, as is the norm).[104]

The FTC has also, on occasion, moved against data brokers. In 2006, a data broker was ordered to pay civil penalties after the FTC alleged that it

96. Brian Fung & Craig Timberg, *The FCC Just Passed Sweeping New Rules To Protect Your Online Privacy*, WASH. POST (Oct. 27, 2016), http://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/ ("But the FCC may have little jurisdiction—or appetite—for regulating the data practices of individual Web companies; Wheeler has repeatedly declined to extend new regulations to the sector.").

97. *Id*.

98. *Cf*. Report and Order on Remand, Declaratory Ruling, and Order, In the Matter of Protecting and Promoting the Open Internet, 30 F.C.C. Rcd. 5601, 5609-10 (2015) ("The open Internet rules . . . apply to both fixed and mobile broadband Internet access service . . . . '[B]roadband Internet access service' (BIAS) . . . is defined to be: A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part." (emphasis removed)).

99. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600, 610 (2014).

100. 15 U.S.C. §§ 45, 52 (2012); *see* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 811 (2011) (tracing the FTC's evolving role in the enforcement of consumer protection).

101. Electronic Privacy Information Center, *In re*: *Snapchat* (last visited Apr. 1, 2017), http://epic.org/privacy/internet/ftc/snapchat/#response.

102. Brett Molina, *Snapchat Settles Privacy Complaint with FTC*, USA TODAY (May 8, 2014), http://www.usatoday.com/story/tech/2014/05/08/snapchat-ftc/8853239.

103. Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

104. *See FTC Data Brokers*, *supra* note 4, at 42.

violated the FCRA by furnishing credit reports to subscribers.[105] More recently, in 2015, the FTC charged data broker Sequoia One with "knowingly selling the financial information of applicants for payday loans to a scam operation that took millions of dollars from consumers by debiting their bank accounts or charging their credit cards without their consent."[106]

However, these actions reflect the outer bound of the FTC's authority to check the activity of data brokers. The FTC may only pursue action against (1) commercial activity that violates existing law, or (2) activity that involves the broker knowingly facilitating crimes.[107] The recent FTC broker report highlights the agency's limited jurisdictional reach—the FTC can "only call for transparency and accountability, they cannot mandate it without supporting legislation."[108] In the case of the sale of consumer data to other consumers, the FTC would not have the authority or justification to allege unfair business practices or any other statutory violation

D. Contractual Restrictions on the Sale of Digital Information

One legal obstacle to the selling of information to individuals stems from certain contractual agreements that individual companies may require when they sell data to brokers. The FTC report noted that companies that sell data to brokers "may also prohibit data brokers from re-using or re-selling data without permission; decoding or reverse engineering the data;" or require "a written agreement affirming that the data broker will only use the data for a specified purpose."[109] However, state and federal statutes do not require these protections, which buyers or sellers self-impose on an individual basis.[110]

III. The Threat of Relational Control

This Part introduces the concept of relational control and explains both (i) how the sale of personal information to individuals can be harmful and (ii) why the sale of consumers' data will likely expand in the coming years.

105. Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. Choicepoint Inc., No. 1:06-cv-00198-JTC (N.D. Ga. Feb. 15, 2006), http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

106. CQ Roll Call Staff, *FTC Cites 2015 Successes in Privacy, Data Security Actions*, 2016 WL 2759289 (Apr. 6, 2016).

107. *Cf*. Lipman, *supra* note 12, at 790 ("If users do not do their homework on what information their apps are collecting about them, and the app makers are not foolish enough to outright lie about what they are doing, the FTC's ability to control how companies share our data is very limited.").

108. *Id*. at 789 (emphasis removed).

109. *See FTC Data Brokers*, *supra* note 4, at 17. For more on how these contractual provisions could be useful hooks to prevent relational control, see *infra* Part V.

110. Emily Steel, *Disparate Network of Companies Is Difficult To Bring to Heel*, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/intl/cms/s/0/a0cb7b5e-d343-11e2-b3ff-00144feab7de.html.

There may be legitimate reasons why a person would want to buy records of another's digital activity, whether to use as a screening mechanism or to increase transparency. However, these possible benefits are not central to this Note's inquiry. This Note highlights a particular problem—relational control—that may accompany the sale of consumer data to individual buyers.

The premise of relational control proceeds from two assumptions. First, certain informational advantages have powerful effects among members of the same social or professional network. Second, these types of information either are[111] or will soon be available for legal purchase.

A. Informational Asymmetries as Tools for Social Influence

Information drives human society. The need for information is why intelligence gathering is an essential tool of statecraft.[112] Even outside of the national security realm, however, all human actions are influenced by a wide array of factors and variables, many of which are indiscernible to both the decision maker and observer.[113] Nevertheless, the more an individual can access relevant data, the more easily that individual can predict the actions of another person or group.

Not all information is useful. A link to a person's Facebook page or public Twitter profile may not provide hidden behavioral insights or the opportunity to influence.[114] However, information that reveals a person's private activity can help explain that person's interests and observable behaviors. In the current digital climate, myriad data types can provide insights about these private dynamics.

In the aggregate, social network data can reveal the "underlying social processes that drive network dynamics, such as the tendency for reciprocity, transitivity, or the need for group balance."[115] A specific person's social

111. There are no confirmed reports in the United States of brokers selling user purchase history, browsing data, or other sensitive information to individual consumers.

112. *See, e.g.*, SUN TZU, THE ART OF WAR (Lionel Giles, trans., 1910), http://classics.mit.edu/Tzu/artwar.html ("Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.").

113. *See, e.g.*, KATHLEEN M. GALOTTI, MAKING DECISIONS THAT MATTER: HOW PEOPLE FACE IMPORTANT LIFE CHOICES 67 (2005) ("People do not have direct introspective access to many of their higher order cognitive processes. That is, they don't always know why they feel or think the way that they do.") (internal reference omitted); Cindy Dietrich, *Decision Making: Factors that Influence Decision Making, Heuristics Used, and Decision Outcomes*, 2 INQUIRIES J. 1-2 (2010) (surveying psychological research on human decision making).

114. *But see* Ashley Feinberg, *This Is Almost Certainly James Comey's Twitter Account*, GIZMODO (Mar. 30, 2017), http://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641.

115. Arun Sundararajan et al., Research Commentary, *Information in Digital, Economic, and Social Networks*, 24 INFO. SYS. RES. 883, 895 (2013).

network data can similarly map that person's interactions[116]—conversations, rivalries, romantic interests, and bitter pasts.[117] An individual's browsing data can reveal what causes that person to feel joyful or stressed, as well as what that person reads, watches, plays, or listens to for information, levity, and distraction. These data capture compulsions, neuroses, and lusts,[118] and help reveal personality flaws and strengths.[119] Biometric data provide even more granularity: wearable technology can capture sleep cycles, the frequency of sexual activity, exercise patterns, and heart rate responses over time—a record of how people's bodies respond to the joys, frustrations, curiosities, and minutiae of day-to-day life.[120]

While the effects of covert access to these data types has not yet been studied, scholars have explored how someone with a favorable access to information are advantaged in a variety of contexts. Researchers studied email traffic in a recruiting firm, finding that "access to information strongly predicts the number of projects completed by each individual and the amount of revenue that person generates."[121] Information access can also provide means to develop productive relationships. In experiments that simulated communications between negotiators, researchers found that bargainers used "informational and relational messages to establish a positive social tenor in the interaction," which facilitated more efficient negotiations.[122] Scholarship has also explored how informational asymmetries provide advantages that can undermine efficiency in markets[123] and influence both peer relationships[124] and broader social networks.[125]

116. *See, e.g.*, Jure Leskovec, *Social Circles: Facebook* (last visited Feb. 18, 2017), http://snap.stanford.edu/data/egonets-Facebook.html.

117. Gregory Ferenstein, *Predicting Love and Breakups with Facebook Data*, TECHCRUNCH (Feb. 14, 2014), http://techcrunch.com/2014/02/14/facebook-love-data/.

118. *See, e.g.*, Wolfie Christl & Sarah Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* 12-17 (2016), http://www.privacylab.at/wp-content/uploads/2016/09/Christl-Networks__K_o.pdf.

119. *Cf.* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (arguing that access to GPS data enabled the state to learn of any citizen's "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on" (internal citations omitted)).

120. *See, e.g.*, Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76 (2016).

121. Sinan Aral et al., *Productivity Effects of Information Diffusion in Networks* 1 (MIT Sloan Sch. of Mgmt. Working Paper No. 4683-08, 2007), http://dspace.mit.edu/bitstream/handle/1721.1/65404/SSRN-id1085354.pdf.

122. Joydeep Srivastava & Dipankar Charkravarti, *Channel Negotiations with Information Asymmetries: Contingent Influence of Communication and Trustworthiness Reputations*, 46 J. MARKETING RES. 557 (2009).

123. *See, e.g.*, Antonio Cabrales et al., *Hidden Information, Bargaining Power, and Efficiency: an Experiment*, 14 EXP. ECON. 133, 134 (2011) (describing how "the theory of markets with asymmetric information has been a 'vital and lively field of economic research,'" which has observed "that asymmetric information led to economic inefficiency, and could even destroy an efficient market" (internal references omitted)); *id.* at 134-37 (reviewing existing scholarship on informational

This Note's opening hypothetical illustrates how asymmetric access to information about another's habits can change the trajectory of conversations, affect what people think and feel, and influence a target's decisions about whom to hire. This is not the only possible example—an informational edge can give an individual the capacity to nudge, manipulate, and ultimately exert control over another person's or group's major decisions.[126]

B. Factors that Suggest Private Consumer Information Will Be Available for Individual Purchase

Relational control is premised on the availability of one's private, information being available for purchase by individual consumers.[127] This information is already being sold.[128] As previously discussed, brokers in other countries have begun selling consumer data that was not already publicly available.[129] Little prevents U.S. brokers from soon doing the same.[130]

In addition, several other factors suggest that the types of information sold in the incipient people search market will increase over the next few years, further exposing consumers to a relational control threat. These factors should raise significant concerns for privacy scholars, lawmakers, and consumers.

asymmetries in business relationships); James E. Parco, *Price-Setting Power and Information Asymmetry in Sealed Bidding*, 27 MANAGE. DECIS. ECON. 413 (2006).

124. *See, e.g.*, Cyril Tomkins, *Interdependencies, Trust and Information in Relationships, Alliances and Networks*, 26 ACCT., ORGS. & SOC'Y 161, 166 n.10, 166-67 (2001) (describing the relationship between information access and trust development in social networks, and the challenges posed by information asymmetries); Nermin Eyuboglu & Osman A. Atac, *Informational Power: A Means for Increased Control in Channels of Distribution*, PSYCHOL. & MARKETING (1991)

125. *See, e.g.*, Nicoleta Bălău & Sonja Utz, Exposing Information Sharing as Strategic Behavior: Power as Responsibility and "Trust" Buttons, 46 J. APPLIED SOC. PSYCHOL. 593 (2016); Jeong Hwang et al., *Information Asymmetry, Social Networking Site Wordof Mouth, and Mobility Effects on Social Commerce in Korea*, 17 CYBERPSYCHOL., BEHAV. & SOCIAL NETWORKING 117 (2014).

126. *Cf.* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009) (arguing on a macro level that experts can offer certain choice architectures that drastically affect consumer decision making).

127. While not the focus of this Note, the possibility of individuals using their professional roles to secure data on others in their network should not be overlooked, as employees at both Facebook and the NSA have, in the past, used their access to view the data of others not outside of professional interest. *See* Bruce Schneier, *Why Uber's 'God View' Is Creepy*, CNN (Dec. 4, 2014), http://www.cnn.com/2014/12/04/opinion/schneier-uber-privacy-issue/index.html ("In the early years of Facebook, employees had a master password that enabled them to view anything they wanted in any account. NSA employees occasionally snoop on their friends and partners. The agency even has a name for it: LOVEINT.").

128. *See GAO Information Resellers*, *supra* note 39, at 3-4 (describing public and proprietary data flows for people search services in the United States).

129. *See supra* notes 2-3.

130. *See generally supra* Part II.

1. The Expansion of Data (and Data Holders)

With each digital advancement over the past 30 years—from internet accessible personal computers, to smartphones,[131] to wearable technologies, and now automated personal assistants[132]—both the type and amount of data that consumers produce has increased dramatically. A similar expansion has occurred with respect to the number of entities—including ISPs, websites, domains, applications, internet-connected devices, and brokers—that control[133] and sell[134] this data. These trends suggest that consumers may soon be able to purchase many new types of personal data.

2. Information Is Cheap

While data brokers make hundreds of millions of dollars in annual revenues, buying personal data in bulk is astonishingly inexpensive.[135] Basic information about a person's age, gender, and location is worth a mere $0.0005 per person.[136] More targeted commercial information—such as persons looking to purchase a car or a vacation—is only marginally more expensive at $0.0021 per person.[137] Marketers will pay $0.11 to know that a woman is pregnant and in her second trimester.[138] While the cost of data increases with the intimacy of the information, the prices per person remain low—$0.26 per person will buy access to lists of people with specific health conditions or taking certain

131. *See GAO Information Resellers*, *supra* note 39, at 22.

132. *See, e.g.*, Ingrid Lunden, *Google Assistant, its AI-based Personal Helper, Rolls out to Nougat and Marshmallow Handsets*, TECHCRUNCH (Feb. 26, 2017), http://techcrunch.com/2017/02/26/google-assistant-its-ai-based-personal-helper-rolls-out-to-nougat-and-marshmallow-handsets (describing the company's "answer to Apple's Siri and Amazon's Alexa").

133. The proliferation of data controllers is modeled compellingly by theDataMap, a research project in Harvard University's Data Privacy Lab. *See, e.g.*, *Survey of Popular Free Apps*, THEDATAMAP (accessed Apr. 18, 2017), http://thedatamap.org/mobile2014/apps.php.

134. *See, e.g.*, *Brian Naylor, Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016), http://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it (describing the observations of former FTC Commissioner Julie Brill, who noted that companies the vast amount of information that companies shared with each other, including "what Web pages we visit, where we're shopping, who we're interfacing with on social media—all of that information is available to be collected by entities that park themselves on the various websites"); Meta S. Brown, *When and Where To Buy Consumer Data (And 12 Companies Who Sell It)*, FORBES (Sept. 30, 2015), http://www.forbes.com/sites/metabrown/2015/09/30/when-and-where-to-buy-consumer-data-and-12-companies-who-sell-it/#6d19b0e73285; *GAO Information Resellers*, *supra* note 39, at 22-27.

135. *See, e.g.*, Emily Steel, *Companies Scramble for Consumer Data*, FIN. TIMES (June 12, 2013), http://www.ft.com/cms/s/0/f0b6edc0-d342-11e2-b3ff-00144feab7de.html; Emily Steel, *Disparate Network of Companies Is Difficult To Bring to Heel*, FIN. TIMES (June 12, 2013), http://www.ft.com/intl/cms/s/0/a0cb7b5e-d343-11e2-b3ff-00144feab7de.html.

136. Emily Steel, *Financial Worth of Data Comes in at Under a Penny a Piece*, FIN. TIMES (June 12, 2013), http://www.ft.com/intl/cms/s/0/3cb056c6-d343-11e2-b3ff-00144feab7de.html.

137. *Id.*

138. *Id.*

prescriptions.[139] Data marketed to individuals is significantly more expensive than bulk data purchases.[140] And while the price will likely vary depending on whether the records are available publicly or purchased from proprietary sources, thus far consumer records of either type have not been prohibitively expensive for interested buyers.[141]

3. Regulators Face Economic and Legal Roadblocks

As noted in Part II, there are few legal obstacles to the purchase and sale of most online activity.[142] The United States' sector-by-sector approach to privacy regulation leaves few general rules governing what people may do with data.[143]

This legal context seems unlikely to change soon. Not only is a dramatic shift of U.S. federal statutory law unlikely, but data sale is an enormous, multi-billion-dollar industry that also provides many positive benefits—including the many free services that are offered online. Any significant change to U.S. privacy law would implicate nearly every commercial industry and constitute a significant departure from longstanding U.S. privacy law. Further, constitutional roadblocks may stymie possible interventions. Many First Amendment scholars assert that data sale likely constitutes protected speech,[144]

139. *Id*. The *Financial Times* released a pricing calculator for a wide array of information about one's demographics, property, family and health information, property, activities, and consumption habits. Selecting all possible price tags yields roughly a rate of $4.8449 per person. *See* Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html.

140. For example, *Everify.com* charges users $19.95 for a premium search, in addition to a 19.95 monthly flat-usage rate. *See supra* note 1. *Spokeo* charges $4.95 per month for a (quota-limited) search of information that is collected from publicly available sources. *See* SPOKEO, http://www.spokeo.com/purchase?pid=32704751121&q=Theodore+Rostow&type=name&url=%2FTheodore-Rostow%2FTexas%2FSan-Antonio%2Fp32704751121.

141. See *Personal Data, supra* note 3 ("[T]he private information of many citizens can be freely purchased by strangers for just 700 yuan, or $101 USD."); Sarkhel & Alawadhi, *supra* note 2 ("For anywhere between Rs 10,000-15,000 [roughly $150-230 USD], we were offered personal data of upto 1 lakh [100,000] people in Bangalore, Hyderabad and Delhi.").

142. *See, e.g*., Neal Ungerleider, *Yes Political Campaigns Follow Your Browser History*, FASTCOMPANY (Nov. 5, 2013, 9:30 AM), http://www.fastcompany.com/3021092/yes-political-campaigns-follow-your-browser-history ("There are few laws preventing marketing firms working on election campaigns (or, for that matter, selling laundry) from leveraging publicly available census and voter registration data and correlating it with things like, say, purchased supermarket loyalty card analytics.").

143. *See, e.g*., *GAO Information Resellers*, *supra* note 39, at 22; *Data Brokers and "People Search" Sites*, PRIVACY RTS. CLEARINGHOUSE (Dec. 16, 2016), http://www.privacyrights.org/content/data-brokers-and-your-privacy ("[T]here are no current federal laws requiring data brokers to maintain the privacy of consumer data unless they use that data for credit, employment, insurance, housing, or other similar purposes. . . . No federal law provides consumers with the right to correct inaccuracies in the data or assumptions made by data brokers." (internal reference omitted)).

144. *See, e.g*., Jane Bambauer, *Is Data Speech*, 66 STAN. L. REV. 57, 106 (2014) ("A corporation that generates and subsequently uses or sells data, even if the revenue stream is ancillary to its primary product or service, has a cognizable argument that it is in the business of communications, and is therefore analogous to a traditional press corporation."); Eugene Volokh, *Freedom of Speech and*

which could prevent legislation that aimed to stop brokers from selling data to consumers. While this Note proposes a number of regulatory, tort, statutory, and private law reforms that would help mitigate the threat of relational control, these are by no means simple or cure-all fixes.

4. Anonymization Is Not a Sufficient Solution

Finally, relational control will likely become a more significant problem due to the well-documented problems associated with data anonymization. Commercial entities and regulators often respond to consumer privacy concerns by attempting to remove all identifying features from a data set.[145] These efforts are pervasive in data transactions. For example, the HIPAA Privacy Rule requires that health data be anonymized,[146] and it creates a safe harbor for companies that (i) remove from datasets eighteen types of identifiers (including, for example, names, addresses, IP addresses, and social security numbers) and (ii) also have "[n]o actual knowledge [that] residual information can identify individual[s]."[147] Similarly, a vast number of companies, including banks,[148] credit cards companies,[149] anti-virus software,[150] telecommunications companies,[151] ISPs,[152] internet companies,[153] and data brokers themselves sell

Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You, 52 STAN. L. REV. 1049, 1051 (2000) (arguing that many privacy laws regulating the sale and disclosure of personal information are unconstitutional under existing First Amendment law).

145. *See, e.g.*, *FTC Data Brokers*, *supra* note 4, at 14.

146. *See* 45 C.F.R. pt. 164.514(b)-(c) (2002).

147. OFFICE OF CIVIL RIGHTS, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 7-8, DEP'T OF HEALTH & HUMAN SERVS. (2002), http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#standard.

148. *See, e.g.*, Jonathan Camhi, *Barclays Plans To Sell Anonymized Data to Other Companies*, BANKTECH (June 24, 2013, 11:32 AM), http://www.banktech.com/data-and-analytics/barclays-plans-to-sell-anonymized-data-to-other-companies/d/d-id/1296436 (announcing Barclay's plans to sell aggregated checking and savings account data to other private companies and government agencies).

149. *See, e.g.*, Bernard Marr, *American Express Charges into the World of Big Data*, DATAINFORMED (Jan. 13, 2016, 5:30 AM), http://data-informed.com/american-express-charges-into-world-big-data (describing new American Express business lines using customer data to recommend third-party products to customers).

150. *See, e.g.*, James Temperton, *AVG Can Sell Your Browsing and Search History to Advertisers*, WIRED (Sept. 18, 2015), http://www.wired.co.uk/article/avg-privacy-policy-browser-search-data (detailing AVG's updated policy to sell anonymized search and browser history).

151. *See, e.g.*, Bryan Clark, *Comcast: ISPs Should Be Able To Sell Your Web History to Advertisers*, TNW (Aug. 3, 2016, 1:09 PM), http://thenextweb.com/insider/2016/08/03/comcast-isps-should-be-able-to-sell-your-web-history-to-advertisers (reporting that AT&T had been selling customer data for over a year); Michael H., *AT&T Planning To Sell Your Anonymous Usage Data to Advertisers*, PHONEARENA (July 3, 2013, 9:37 PM), http://www.phonearena.com/news/AT-T-planning-to-sell-your-anonymous-usage-data-to-advertisers_id44890 (announcing AT&T plans to sell anonymized customer data).

152. Swati Khandelwal, *ISPs Sell Your Data to Advertisers, But FCC Has a Plan To Protect Privacy*, HACKER NEWS (Mar. 11, 2016), http://thehackernews.com/2016/03/isp-sells-data-to-advertisers.html; *supra* note 57.

data to other companies after stripping out personally identifiable information (PII).[154]

However, anonymization cannot guarantee that a person is not tied to their data, according to many computer scientists, data analysts, and privacy scholars.[155] Surveys of common anonymization and de-anonymization methods reveal the ease with which computers and humans can re-identify anonymized datasets. For data releases that are explicit (intentional, such as when anonymized and sanitized datasets are sold) or implicit (unintentional, such as when partially or fully anonymized datasets are leaked),[156] a number of de-anonymization attacks can re-identify the datasets with ease.

A particularly effective attack (and relevant to our inquiry) involves the attacker leveraging auxiliary information or background knowledge to identify the matching dataset.[157] For example, Arvind Narayanan and Vitaly Shmatikov took user ratings from the IMDB database and used them to expose user IDs from among 500,000 Netflix users.[158] Working off the hypothesis that among "Netflix subscribers who also use IMDB, there is a strong correlation between their private Netflix ratings and their public IMDB rating," Narayanan and Shmatikov discovered that "even a handful of movies that are rated by a subscriber in both services would be sufficient to identify his or her record in the Netflix Prize dataset (if present among the released records) with enough statistical confidence to rule out the possibility of a false match except for a negligible probability."[159] In addition, Sarah Jamie Lewis has surveyed how a 20GB dataset, comprising more than 173 million individual New York City

153. *See e.g.*, Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, PROPUBLICA (June 11, 2011, 11:45 AM), http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you (describing the types of information sold by internet companies to political campaigns).

154. *See id*. ("[T]he credit reporting giant Experian performs a 'double-blind' match between Microsoft's data and campaigns' data. Yahoo uses another massive data company, Acxiom. Both Experian and Acxiom also offer similar matching for commercial clients who want to find previous customers online.").

155. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) ("Although it is true that a malicious adversary can use PII such as a name or social security number to link data to identity, as it turns out, the adversary can do the same thing using information that nobody would classify as personally identifiable."); Scott Berinato, *There's No Such Thing as Anonymous Data*, HARV. BUS. REV. (Feb. 9, 2015), http://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data ("Broadly, it means that anonymity doesn't ensure privacy, which could render toothless many of the world's laws and regulations around consumer privacy.").

156. *See* Bin Zhou et al., *A Brief Survey on Anonymization Techniques for Privacy Preserving Publishing of Social Network Data*, 10 ACM SIGKDD EXPLORATIONS NEWSL. 12 (2008), http://www.cs.sfu.ca/~jpei/publications/SocialNetworkAnonymization_survey.pdf.

157. Xuan Ding et al., *A Brief Survey on De-anonymization Attacks in Online Social Networks*, 2010 INT'L CONF. ON COMPUTATIONAL ASPECTS OF SOC. NETWORKS 611, 614.

158. Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* EEE SYMPOSIUM ON SECURITY AND PRIVACY (S&P) (2008), http://www.cs.cornell.edu/~shmat/shmat_oak08netflix.pdf.

159. *Id*. at 8.

taxi trips with anonymous licenses, medallion numbers, and other metadata could easily be subsequently re-identified along with the driver's identity.[160]

Further, existing relationships pose additional challenges for effective anonymization. Felix Wu describes the possibility of privacy invasions by "insiders" in the context of data releases.[161] Wu defines "privacy 'insiders' [as] those [whose] relationship to a particular individual allows them to know significantly more about that individual than the general public does."[162] Wu notes that privacy insiders can be particularly difficult to counter, because insiders "can exploit special knowledge gained through their relationships with a target individual to deduce more about that individual from released data than the general public would."[163] Similarly, Swaroop Poudel observes how, in the context of anonymized device data,[164] knowledge of a person's particular attributes can lead to identifying an individual without access to their PII.[165] While privacy insiders may interact with each other in the physical world with varying degrees of closeness and trust, their existing knowledge of a person can pair with acquired data to produce greater insight.

These four factors suggest that the threat of relational control will continue to grow. Consumers produce increasingly revealing data, which brokers will continue to sell at a low price. Economic and legal obstacles may frustrate attempts to regulate data sales, and anonymization cannot adequately protect consumers. In the absence of any meaningful check, certain individuals will purchase cheap, powerful data to gain an informational advantage over their peers.

IV. Existing Proposals Fail To Remedy Relational Control

This Part examines the prominent reforms that privacy scholars have proposed to address privacy harms that stem from the sale of digital information.

160. Sarah Jamie Lewis, *Please Stop Releasing "Anonymized" Datasets*, LINKEDIN PULSE (Jan. 25, 2016), http://www.linkedin.com/pulse/please-stop-releasing-anonymized-datasets-sarah-jamie-lewis.

161. *See* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1154 (2013). While Wu underscores the unclear legal state of insider attacks, and their difficulty to counter, neither Wu nor any other scholar has discussed the possibility or implications of these relationships in the context of peer data purchases.

162. *Id*.

163. *Id*.

164. *See also infra* Section III.B (discussing the relationship between de-anonymization and a relational control threat).

165. Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L. J. 997, 1014 (2016) ("Comprising granular data with many variables, sensor data can enable someone with knowledge of certain attributes of a person to identify them, even without their personally identifiable information (PII) . . . . For example, Fitbit's movement data can reveal someone's gait. Someone who knows a person's gait could, thus, identify that person and gain access to the rest of his or her Fitbit data." (internal references omitted)).

A. Broker Industry Reforms

When the FTC released its 2014 Report, the agency proposed a series of legislative reforms that, if enacted, would offer new privacy protections for consumers. The FTC signaled its support for the Data Broker Accountability and Transparency Act (DATA), introduced by Senators Rockefeller and Markey, which would (1) bar data brokers from collecting data that brokers knew were illegally obtained; (2) require brokers to allow consumers to review personal information gathered about them at least once per year for free; and (3) empower consumers to dispute the accuracy of data collected, which brokers would then have to investigate and correct.[166] The FTC also expanded upon the existing DATA proposals by recommending legislation that would require consumers to *opt in* to the sharing of any sensitive data, such as certain health data.[167] The FTC also recommended that the legislation require brokers to disclose their data sources and notify consumers when collected data adversely affected a commercial transaction.[168] In addition, the FTC suggested that a central website be created to list the largest fifty data brokers and provide links to their access tools and opt-out policies.[169]

A number of privacy scholars have proposed additional reforms to regulate broker activity. These range from the advocating for legislation in line with the EU's Data Privacy directive[170] to expanding disclosure and correction requirements.[171] Scholars have called for Congress to enact a law similar to California's Right to Know Act, which would require companies to reveal, upon request, the information they have collected about an individual and how the information is used and sold.[172]

A recent empirical study of consumer reactions to privacy disclosures registers one critique of these proposals, arguing that they "rely[] on the fiction that if customers are told about the uses of their information, they will vote with their feet if they do not like the terms."[173] However, the novel proposals

166. *See* Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014); Schmitz, *supra* note 12.

167. *Id*. at 52. For more on sensitive data frameworks as a possible response to the threat of relational control, see *infra* Part V.

168. *FTC Data Brokers*, *supra* note 4, at 51-52.

169. Schmitz, *supra* note 12, at 1458.

170. *See, e.g*., Kuempel, *supra* note 12; Maeve Z. Miller, Note, *Why Europe Is Safe from Choicepoint: Preventing Commercialized Identity Theft Through Strong Data Protection and Privacy Laws*, 39 GEO. WASH. INT'L L. REV. 395 (2007). While these and other scholars have called for a more European approach to digital privacy in the commercial realm, this Note takes the view that these calls are unlikely to succeed, given the relative inelasticity of U.S. privacy law in the face of dramatically increased concern over data privacy. *See* Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 347 (2016).

171. *See* Lipman, *supra* note 12, at 786-96.

172. *See, e.g*., Jugpreet Mann, Note, *Small Steps for Congress, Huge Steps for Online Privacy*, 37 HASTINGS COMM. & ENT. L.J. 365, 387 (2015).

173. P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 347 (2016).

offered by the authors—including the creation of Profile Information Reporting Agencies, which, like credit reporting agencies, would store consumers' data profiles and allow consumers to challenge and correct inaccurate information—also would not protect consumers from the threat of relational control.[174]

B. Reforms for Information Services

In addition to the proposals to regulate the data broker industry, scholars have recommended a number of interventions that would require information services and data holding companies to protect consumer privacy. As FTC Chairwoman Edith Ramirez noted, these proposals are usually familiar.[175] Calo and others have proposed that companies offer a tracking-free version of their service that consumers can purchase.[176] Many, including members of Congress, have called instead for the creation of universal "opt-out" provisions for consumers to refuse online tracking.[177] Similarly, many scholars have proposed reforms to the increasingly dated statutory privacy protections described in Part II.[178]

Scholars also typically line up behind (or critique) various "good data practices" frameworks, such as the Fair Information Practice Principles (FIPPs) framework.[179] The FTC articulated its Privacy By Design (PBD) principles in 2012, which call on companies to delete consumer data that are no longer needed and to allow consumers to access their data and, when appropriate, to change or delete information that companies possess.[180] These principles are neither wholly novel[181] nor without criticism, including ideological

174. *See id*. at 346-49.

175. Edith Ramirez, Chairwoman, FTC, *The Privacy Challenges of Big Data: A View from the Lifeguard's Chair* 1 (Aug. 19, 2013), http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf ("The emergence of big data is similarly breathtaking and potentially game changing. But the challenges it poses to consumer privacy are familiar . . . . The solutions are also familiar.").

176. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 95 (2014).

177. *See* Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011); Do-Not-Track Online Act of 2011, S.913, 112th Cong. (2011); Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information,* 74 WASH. L. REV. 1033 (1999).

178. Eugene E. Hutchinson, Note, *Keeping Your Personal Information Personal: Trouble for the Modern Consumer*, 43 HOFSTRA L. REV. 1151 (2015); Mann, *supra* note 172, at 37; *See* Ohm, *supra* note 16, at 1191; *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016).

179. Borgesius et al., *supra* note 29, at 2101-06 (describing various Fair Information Principles and how they came to be articulated).

180. *Id*. at 23-24.

181. *See* Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. ECON. & POL'Y 1, 1-2 (2015) (describing the PBD framework as "essentially a restatement of the traditional Fair Information Practice Principles (FIPPs) of Notice, Choice, Access and Security," which in turn embody "all of the concepts" in the 1980 privacy guidelines promulgated by the

disagreement over the scope of consumer protection regulations[182] and the never-ending struggle to keep frameworks up-to-date with the rapid expansion of data and how they are used.[183]

Regulatory FIPP or PBD frameworks are similarly incapable of protecting consumers from relational control. These frameworks, along with coherent cyber security norms,[184] can provide useful best practices for how companies should de-identify and secure data, as well as delete data over time. However, they do not address the basic structural feature of the commercial data environment that allows many private actors to collect records of user activity and sell them to interested purchasers.

Furthermore, it is unlikely that Congress will amend federal privacy statutes either to prevent the trading of the digital information that relates to regulated sectors[185] or to establish general privacy rules for consumer information (as some have recommended).[186] Federal statutory privacy law has remained unchanged despite the rampant purchase and sale of data, a near constant stream of embarrassing data breaches and leaks, and an increasingly lengthy list of documented privacy harms.[187] With one narrow exception,[188] Congress has not passed a statute expanding federal privacy protections in more than a decade.[189] Federal statutory reforms are also often poorly designed to combat future privacy threats. New Congressional enactments would face familiar undertows in the form of swift obsolescence, dilution by industry lobbying, or the well-documented tendency to target specific technologies.[190]

Organization of Economic Cooperation and Development (OECD)); *see also* Borgesius et al., *supra* note 29, at 2101-06 (describing the scope of the OECD guidelines).

182. *See, e.g.*, Paul H. Rubin, *Regulation of Information and Advertising*, 4 COMPETITION POL'Y INT'L 169, 169-92 (2008) (arguing that the FTC has at times overprotected consumers with excessive regulation that curbs innovation).

183. *See, e.g.*, Lenard & Rubin, *supra* note 181, at 26 (arguing that the commissioner's recommendation are "ill suited to the world of big data"); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217 (2013).

184. *Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH. (Feb. 12, 2014), http://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

185. If Congress did reform existing statutes, other records of digital activity, such as what consumers read and watch, would not be affected.

186. *See, e.g.*, Kuempel, *supra* note 12, at 207; Miller, *supra* note 170, at 395.

187. *See generally* Introduction, *supra*.

188. *See* Genetic Information Nondiscrimination Act of 2008, H.R. 493, 110th Cong. § 2 (2008).

189. *See* Ohm, *supra* note 16, at 1125 (citing the Genetic Information Nondiscrimination Act as the only "meaningful expansion of privacy law Congress has enacted in the last decade").

190. *See* Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J.L. & TECH. 24 (2012) (documenting examples of statutes that prove ineffective or stifling because they target particular technologies for reform).

C. Privacy-Enhancing Consumer Technologies

Technologists have developed a number of tools to shield consumers from digital tracking, such as adblockers or cookie deleting services. However, these services are unlikely to inoculate a user from the threat of relational control. There are significant economic incentives for online actors to track consumer activity,[191] which fuel the internet's free pricing structure.[192] These incentives lead to new tracking technologies (such as web beacons),[193] which when first implemented track consumers without their knowledge, and new services (such as Pokémon Go), which often begin with few privacy protections for consumers.[194] This lag time is an inevitable consequence of a free market economy, and ensure that technical opt-outs will struggle to provide sustained protection against relational control.

Additionally, a wide array of tools—from the Tor browser,[195] to virtual private networks (VPN),[196] end-to-end encrypted messages,[197] and encrypted

191. *See* Alan Henry, *Everyone's Trying To Track What You Do on the Web: Here's How To Stop Them*, LIFEHACKER (Feb. 22, 2012, 8:00 AM), http://lifehacker.com/5887140/everyones-trying-to-track-what-you-do-on-the-web-heres-how-to-stop-them; Meghan Neal, *Now You Can See Which Websites Are Tracking You in Real-Time*, MOTHERBOARD (Oct. 25, 2013, 9:35 AM), http://motherboard.vice.com/blog/now-you-can-see-what-websites-are-tracking-you-in-real-time.

192. *See, e.g.*, Lipman, *supra* note 12, at 778 ("If you search for something on the Center for Disease Control's website, say, 'herpes symptoms,' then the CDC will tell Google about your search. The CDC is not trying to profit from you, but they use Google Analytics to measure their website traffic. The CDC uses Google Analytics because it is an effective free tool. It is a 'free' tool because it is quietly paid for with your data." (internal citations omitted)); Emily Steel, *Companies Scramble for Consumer Data*, FIN. TIMES (June 12, 2013, 8:11 PM); *How Many of Your Users Set "Do Not Track"?*, QUANTABLE (Feb. 2, 2015), http://www.quantable.com/analytics/how-many-do-not-track/ (measuring the percent of users who opt out of tracking as between 8% and 15%). *But see* Joseph Turow, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*, U. PENN (June, 2015), http://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

193. Joanna Geary, *Tracking the Trackers: What Are Cookies? An Introduction to Web Tracking*, GUARDIAN (Apr. 23, 2012) (describing flash cookies and web beacons).

194. *See, e.g.*, Brian Barret, *Update Your Pokémon Go App Now To Fix That Privacy Mess*, WIRED (July 12, 2016), http://www.wired.com/2016/07/update-pokemon-go-app-now-fix-privacy-mess ("That means it could have potentially been able to 'see and modify nearly all information in your Google Account,' according to Google, short of changing your password or tapping into Google Wallet. This is very bad! And now you can fix it.").

195. *See, e.g.*, Kavita Iyer, *Best Free Tools for Anonymous Browsing 2016*, TECHWORM (May 21, 2016), http://www.techworm.net/2016/05/top-free-tools-2016-anonymous-browsing.html.

196. *See, e.g.*, Adi Robertson, *A VPN Can Stop Internet Companies from Selling Your Data—But It's Not a Magic Bullet*, THEVERGE (Mar. 30, 2017), http://www.theverge.com/2017/3/25/15056290/vpn-isp-internet-privacy-security-fcc-repeal ("The right VPN can protect against lots of things, including government surveillance and malware. But the tool isn't a magic privacy bullet—in fact, experts can't even agree on a great VPN service, beyond one you make yourself. While a huge number of companies provide VPNs, many have potential security flaws or could put your data at risk. It's also difficult to tell how secure a VPN actually is, and what it's doing with your data. So what are you supposed to do if you want to use one? The short answer is to avoid free services, and if you consider yourself tech-savvy, look into setting up your own. Otherwise, make sure a paid VPN has a privacy policy you're okay with, and can handle the threats you're relying on it to protect you from.")

desktops[198]—allow consumers to avoid tracking by most companies and some security agencies. Most websites run considerably slower on the Tor browser, and some features, including most video streaming options, cannot work without risking consumer privacy.[199] While certain, high information consumers could limit their vulnerability from relational control, most consumers will not take the steps necessary to shroud their activity.[200] (And, if they did, their actions could significantly disrupt the information economy.)[201]

V. "Information Fiduciaries" and "Sensitive Data": Promises and Limits

While most proposed reforms would offer minimal protection against relational privacy harms, two scholars—Paul Ohm and Jack Balkin—recently proposed new frameworks that could better protect consumers. This Part lays out both proposals and describes how each could be amended or extended to enhance consumer protection against the threat of relational control.

A. Two Approaches to Consumer Protection

Ohm and Balkin tackle data abuses from two distinct fronts, each of which is relevant to the problem of relational control. Ohm's proposal is *data-centric*, highlighting particular types of information—such as social security numbers or medical information—that can harm consumers and, thus, are recognized as "sensitive." Legal safeguards exist for certain types of "sensitive" information, which limit how commercial entities may use these data.[202] Ohm advocates expanding U.S. law's conception of sensitive data to include three new types of information: precise geolocation data, remote biometric data, and communications metadata.[203]

197. *See, e.g.*, Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police.

198. *See, e.g.*, *Privacy for Anyone Anywhere*, TAILS (last visited Feb. 18, 2017), http://tails.boum.org/ (providing a free encrypted operating system that users can load onto computers and storage devices).

199. *See NoScript* (last visited Apr. 1, 2017), http://noscript.net/ (providing a Firefox extension that blocks scripts from loading on untrusted websites).

200. *See* Kesan, *supra* note 170.

201. *See, e.g.*, John E. Dunn, *Best 7 Online Privacy Tools 2016 – VPNs, Anonymous Search, and Browser Secrecy*, TECHWORLD, (last visited Apr. 1, 2017), http://www.techworld.com/security/best-7-online-privacy-tools-2016-vpns-anonymous-search-browser-secrecy-3633529/ ("If it was only advertisers, privacy would be challenging enough but almost every popular free service, including search engines, social media, cloud storage and webmail, now gathers intrusive amounts of personal data as a fundamental part of its business model.").

202. Regulatory interventions that protect sensitive information include the HHS's HIPAA anonymization rules and the FTC's COPPA rule, which enumerates in its definition of sensitive information a user's first and last name, address (including street name and name of city or town and telephone number). *See* 45 C.F.R. pt. 164.514(b)-(c) (2002); 16 C.F.R. pt. 312 (2014).

203. *See* Ohm, *supra* note 16, at 1143-44.

Balkin's proposal, on the other hand, is *entity-centric*, and offers a new set of limits on what certain data controllers may do with the consumer data entrusted to them. Entities like commercial ISPs and popular applications control vast quantities of information that they have, at times, used to harm or manipulate consumers.[204] Balkin argues that these commercial entities should be understood as "information fiduciaries" that owe duties to their consumers. The duties that Balkin sketches would prevent these entities from using data in ways that *directly* harmed the consumers that entrusted their data to them.

As presently constituted, neither approach offers meaningful protection against relational control. Ohm's conception of sensitive data is too narrow and overlooks myriad information that could be used to manipulate consumers. Balkin's conception of harmful activity misses the possibility that the sale of information can pose an *indirect* threat of consumer harm. Nevertheless, each proposal provides a coherent framework that could better protect consumers from relational control.

B. Sensitive Data and Relational Control: Novel Protections and Conceptual Gaps

Ohm describes sensitive information as a "showstopper"[205] that can summon robust protections out of otherwise lax privacy regulations, if data are sufficiently sensitive.[206] For example, concern for sensitive data is observable in the FTC's recommendation that data brokers establish *opt-out* provisions for most data, but *opt-in* protections for particular, sensitive data.[207] A sensitive data approach to consumer privacy is particularly appealing in light of the few limits that U.S. privacy law places on the sale of digital information. A key feature of the "sensitive information" movement is that it frequently spurs statutory and regulatory action,[208] while also being fueled by private industry.[209] Trade groups, like the Network Advertising Initiative and the Digital Advertising Alliance, and major companies offer their own (often divergent)[210] guidelines on what information is sensitive and, unlike normal data, cannot be sold for profit.[211] Noting these features, Ohm observes that, for

204. *See, e.g.*, *supra* notes 19-20 and accompanying text.

205. Ohm, *supra* note 16, at 1129.

206. *Id*.

207. *FTC Data Brokers*, *supra* note 4, at 54.

208. *See supra* note 202 and accompanying text.

209. Ohm, *supra* note 16, at 1138 ("[Private industry actors] are probably motivated to draw these lines by a combination of moral compunction, ethical norms, market demand, and fear of consumer backlash or government regulation.").

210. *See, e.g.*, *id*. at 1138-40; Jim Brock, *Yet Another (Better) Definition of Sensitive Boundaries for Ad Targeting*, PRIVACYCHOICE (Dec. 14, 2011), http://blog.privacychoice.org/2011/12/14/yet-another-better-definition-of-sensitive-boundaries-for-ad-targeting (arguing that the various different industry standards for sensitive boundaries should coalesce along the lines of Google's definition).

211. *See* Ohm, *supra* note 16, at 1138-40.

privacy advocates, sensitive data "may be the only game in town"[212] that can secure protections where so many other proposals have failed.

1. Possible Protections Against Relational Control

A number of Ohm's proposals, if implemented, could yield value in the looming fight against relational control. First, Ohm's three new types of "sensitive" data—precise geolocation data, remote biometric data (including iris scan and facial recognition), and communications metadata[213]—are particularly dangerous in the context of relational control. Communications metadata can offer powerful maps of an individual's social networks and reveal changes in interactions.[214] For example, Facebook communications metadata can predict with surprising confidence when individuals will begin a romantic relationship.[215]

Second, Ohm argues that U.S. law should evolve to categorize certain types of data as sensitive data "no matter who holds it."[216] A core challenge for sensitive data as a partial remedy to relational control is that the vast majority of relevant U.S. law requires only "particular actors in particular sectors" to have any safeguarding responsibilities for the information.[217] As discussed in Part II, the constant trading of data[218] weakens most U.S. sensitive data laws.[219] Ohm calls for a significant expansion of U.S. law, arguing that for certain types of sensitive information, "we should extend privacy protection regardless of the specific relationship."[220]

Third, Ohm argues that U.S. laws should recognize sensitive data even when in unstructured forms. Unlike structured data that contain only one type of information, like an email address, unstructured data exist "at the whim of the person doing data entry—'comments' or 'notes.'"[221] For example, Google maintains a collection of every search query anyone has entered, which is perhaps the world's largest database of incidentally collected sensitive information.[222] While technical capacity has traditionally limited one's capacity

212. *Id*. at 1136.

213. *Id*. *at* 1143-44.

214. Leskovec, *supra* note 116.

215. *See* Robinson Meyer, *When You Fall in Love, This Is What Facebook Sees*, ATLANTIC (Feb. 15, 2014), http://www.theatlantic.com/technology/archive/2014/02/when-you-fall-in-love-this-is-what-facebook-sees/283865.

216. Ohm, *supra* note 16, at 1190.

217. *Id*.

218. *See* Christl & Spiekermann, *supra* note 118, at 45-50 (surveying major studies of data transmissions that found that "37 of the 50 most popular websites transferred information about every click to over 30 third parties, 22 of them even to more than 60 third parties. The website dictionary.com transmitted data on every page request to 234 external services" (internal references omitted)).

219. *See supra* Section II.A.

220. *Id*. at 1192.

221. *Id*. at 1192-93.

222. *Id*. at 1193.

to retrieve valuable or tailored information from massive, unstructured datasets like Google's, the rapidly expanding state of computational power, along with an array of web scraping, natural language processing, and machine learning tools,[223] enable companies to capture and separate sensitive data from vast, unstructured collections. Google researchers, for example, have used machine-learning techniques to automatically distinguish flu symptoms from other search queries analyzed from the "billions of individual searches from 5 years of Google web search logs."[224] The power of these new tools underscores the need to consider possible affirmative protection requirements on unstructured data.

2. Significant Gaps with Respect to Relational Control

If implemented, these three proposals might reduce certain manifestations of relational control. Nevertheless, Ohm's proposal is not designed with relational control in mind. As presently constituted, it can provide only marginal protection against the threat of relational control.

Ohm's proposals do not address many information types that can be used to exert relational control. Data that provide deep insights into both behavior and interactions—for example, browser history, calendar data, purchase records, and social network metadata—are particularly dangerous in the hands of peers. To protect against or manage the risk of relational control, Ohm's proposal would need to be significantly expanded to include as sensitive a much larger body of data. Recognizing these data types as sensitive could trigger new regulatory requirements, limiting the circumstances in which this information could be transferred through, among others, the FIPPs of "purpose specification" and "use limitation," which can reduce the likelihood that sensitive data will wind up in the hands of data brokers who are in turn free to sell data to individual consumers that cannot show a valid purpose.[225]

C. Information Fiduciaries and Relational Control: A Theoretical Path To Improve Sale and Storage Practices

Like Ohm, Balkin also looks to jumpstart privacy scholarship by arguing that a fiduciary relationship[226] exists between consumers and data holders.

223. *See id*. at 1194; Liane Colonna, *A Taxonomy and Classification of Data Mining,* 16 SMU SCI. & TECH. L. REV. 309, 332-34 (2013).

224. Ohm, *supra* note 16, at 1195 (quoting Jeremy Ginsberg et al., *Detecting Influenza Epidemics Using Search Engine Query Data,* 457 NATURE 1012, 1013 (2009)).

225. *Id*. at 1138.

226. Other scholars have also proposed some fiduciary obligations for information services. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 282 (2015); Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 812, 831-32 (2012); Kenneth C. Laudon, *Markets and Privacy*, COMMS. ACM 92, 101 (Sept. 1996). *See generally* Richard R.W. Brooks, *Knowledge in Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW (Andrew S. Gold & Paul B. Miller eds., 2014).

Balkin argues this relationship, like other fiduciary relationships, can be regulated[227] without violating freedom of contract[228] or the First Amendment.[229]

Balkin analogizes information services and service providers[230] to doctors and lawyers, who owe a common-law duty of loyalty and confidentiality to their clients and patients.[231] Balkin proposes that certain duties of loyalty and care attach to a wide array of entities, "includ[ing] bookstores, search engines, ISPs, email providers, cloud storage services, providers of physical and streamed video, and websites and social networks when they deal in our intellectual data" (information fiduciaries).[232] Under Balkin's framework, each of these entities would owe consumers some degree of fiduciary obligations when controlling their data.[233]

As with Ohm's sensitive data proposal, Balkin's information fiduciaries framework is ill-suited as proposed to protect consumers from relational control. Balkin's framework is designed to protect consumers from direct ill treatment by the companies that initially collect their data,[234] rather than from the indirect relational abuses that data transactions enable. Balkin does not explore whether and how to extend fiduciary obligations to data sale. Concerned that such obligations would undermine the financial viability of information services,[235] Balkin also disputes, at least to some extent, the idea

227. *See* Balkin, *supra* note 19, at 1205 ("The idea of fiduciary duties gives us a way out of the neo-Lochnerian model that binds First Amendment freedoms to contractual freedom. It also offers us a way of explaining why certain kinds of information are matters of private concern that governments can protect through reasonable regulation. My central point is that certain kinds of information constitute matters of private concern not because of their *content*, but because of the *social relationships* that produce them.").

228. A major dilemma raised in privacy scholarship is how to treat a company's privacy policy, and to what extent the privacy policy should be understood as a contract that binds both consumers to (often-unconsidered) agreements and companies to prior promises of privacy. *See, e.g.*, M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere),* 87 NOTRE DAME L. REV. 1027 (2012); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1880 (2013); Sovern, *supra* note 177.

229. *See, e.g.*, Volokh, *supra* note 114, at 1051 (arguing that many privacy laws regulating the sale and disclosure of personal information are unconstitutional under existing First Amendment law).

230. *Compare* Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,738, 19,741 (Apr. 13, 2015) (defining a broadband internet access service) *with* Telecommunications Act of 1996, Pub. L. No. 104-104, § 3(a)(2), 110 Stat. 56, 58-60 (1996) (codified at 47 U.S.C. § 153(24)) (defining an information service).

231. Balkin, *supra* note 19, at 1205.

232. *Id.* at 1221 (quoting NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 282 (2015)).

233. Balkin does not specify the exact scope of these obligations, which may also differ depending on the information fiduciary's commercial activities. *See, e.g.*, Balkin, *supra* note 19, at 1228.

234. *See, e.g.*, *id.* at 1187-94 (describing a recent Facebook study aimed at manipulating the voting preferences of its users).

235. *See id.* at 1227 ("It cannot be the case that the basic business model of free or subsidized online services inherently violates fiduciary obligations and therefore can be made illegal. 'Fiduciary' does not mean 'not for profit.'").

that fiduciary obligations should trigger liability for possible, indirect harms to end-users.[236]

Nonetheless, Balkin's framework can be extended to combat the threat of relational control without threatening the basic viability of a free services model. The responsibilities of information fiduciaries could be expanded to limit what data companies can sell to brokers and, in particular, the terms of these agreements. The 2014 FTC report notes that some data sellers demand consumer protections in their contracts with brokers.[237] Contractual provisions, if consistently applied across most information services and service providers, could protect consumers to a significant degree from the possibility of relational control. Unlike many other harms associated with data broker practices,[238] relational control becomes a possibility when data brokers sell consumer information to individuals. Accordingly, restrictions on subsequent sales, re-identifying anonymized data, and the use of data beyond a specified set of purposes could meaningfully limit the ability of interested consumers to purchase data.

While Balkin does not discuss how or if fiduciary obligations might extend to data sales, his fiduciaries framework could credibly be extended to obligate companies to store data securely, and restrict what third parties and data brokers may control, sell, and use. A broader construction of fiduciary obligations that extends to data sale and storage does not stretch Balkin's model beyond its intended scope, as restrictions on what data can be sold are included among the fiduciary obligations for doctors and lawyers and, more importantly, are consistent with the general implicit and explicit assurances that information fiduciaries make to consumers that they may be trusted with consumer data.[239]

VI. Doctrinal Recommendations in Light of Relational Control

Protecting consumers from relational control presents a considerable challenge, given the inflexible state of U.S. privacy law and the legal challenges posed by both the First Amendment and contract law. Further, because the threat of relational control both emerges from a wholly legal activity (data purchase) and is the manifestation of quintessential human instincts (to learn about one's peers and make choices based on that information), there is no single answer to this threat that remains consistent with U.S. law. Part VI offers some initial doctrinal recommendations to protect consumers from the threat of relational control. As these proposals are the first to respond to the relational control harm, they are not exhaustive and unlikely

236. *See id*. ("Nevertheless, if we impose fiduciary obligations that are too broad, it might follow that online service providers could not make any money at all from this data because the data might be used in some way to some end-user's disadvantage.").

237. *See FTC Data Brokers, supra* note 4, at 16-17.

238. *See supra* Introduction.

239. *See* Balkin, *supra* note 19, at 1203-05.

to offer a comprehensive solution. This Note invites follow-up proposals and remedies in the years ahead.

A. Congressional Privacy Reforms

Congress should pass legislation that unambiguously protects consumers from a significant relational control threat: the content and meta-data of electronic communications. The SCA prohibits providers of electronic communications services (ECS) from divulging the contents of communications to private parties while those communications are "in electronic storage."[240] It also prohibits providers of a remote communications service (RCS) from divulging the contents of communications "carried or maintained on that service."[241] However, these prohibitions contain significant gaps. The SCA allows entities that qualify as neither ECS nor RCS to disclose communications to third parties,[242] as well as ECS providers to disclose the content of communications that are not in electronic storage.[243] Additionally, the SCA offers no protections for the metadata associated with the content of communications.[244]

Congress should close these gaps by passing legislation that prohibits any person or entity from disclosing, without consent, to non-governmental persons and entities the content and metadata of other forms of electronic communication. Already, there is political interest in some of these reforms. In 2016, the House of Representatives passed the Email Privacy Act, 419-0.[245] The House Bill amends 18 U.S.C. § 2702 to bar (1) an ECS from selling to third parties the content of any communication "that is in electronic storage with or otherwise stored, held, or maintained by that service," and (2) an RCS from selling to third parties the content of any communication communications "that is stored, held, or maintained by that service."[246] This language expands the scope of the SCA to protect the content of all wire and electronic communications that are controlled by an ECS or RCS.

240. 18 U.S.C. § 2702(a)(1) (2012).

241. 18 U.S.C. § 2702(a)(2) (2012).

242. *See* Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997) ("Thus, a person who does not provide an electronic communication service (like Ferguson and Hudson) can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.").

243. *See* Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (holding that emails "were not in electronic storage" after plaintiff "left the single copies of his e-mails on the Yahoo! server and apparently did not download them or save another copy of them in any other location").

244. *Cf*. 18 U.S.C. § 2702(a)(3) (2012) (prohibiting an ECS or RCS from "knowingly divulg[ing] a record or other information pertaining to a subscriber . . . to any government entity").

245. H.R. 699, 114th Cong. (2016), http://www.congress.gov/bill/114th-congress/house-bill/699/text; Dustin Volz, *Email Privacy Bill Unanimously Passes U.S. House*, REUTERS (Apr. 27, 2016, 4:56 AM), http://www.reuters.com/article/us-usa-congress-email-idUSKCN0XO1J7.

246. H.R. 699, 114th Cong. § 2(a)(1)(A)-(B) (2016).

The Email Privacy Act does not currently impose any restrictions on any person or entity that does not qualify as an ECS or RCS but nonetheless might somehow acquire electronic communications. The Email Privacy Act also does not address the sale of metadata—which can provide clear maps of social relationships and how they evolve over time. When the Senate next considers the Email Privacy Act, it should (1) amend the proposed legislation to move away from an entity-centric regulatory model with respect to the sale of communications, and (2) adopt new protections against the commercial sale of metadata. Such an amended Email Privacy Act would provide meaningful protection against the abuse of a particularly dangerous type of data. The law would also reflect both Congress's longstanding preference for narrow privacy reforms and longstanding U.S. commitment to the privacy of written expression.[247]

Congress could make an array of changes to existing federal statutes and, as a result, meaningfully limit (but not eliminate) the threat of relational control.[248] However these changes are unlikely, due to the fact that data sale has become such an important part of the internet economy, the difficulty inherent in mounting a major lobbying campaign,[249] and that Congress is likely to prioritize privacy reforms in the national security space in the near term over those in the commercial sphere.[250] Additionally, while updating existing privacy rules in laws such as HIPAA and FERPA would likely prove beneficial, it could also have unintended negative effects on the economy, removing a significant income stream from free applications and sites that collect data related to one's health or education.[251]

B. Privacy Torts Reconsidered

Common law courts could also provide an ex post remedy for victims of relational control and related privacy harms by extending existing privacy and negligence torts to reflect contemporary technological sensibilities.

247. *See* 18 U.S.C. § 1702 (2012) ("Whoever takes any letter, postal card, or package [of another] . . . or opens, secretes, embezzles, or destroys the same, shall be fined under this title or imprisoned not more than five years, or both.").

248. *See generally supra* Parts II & IV.

249. *See, e.g.*, Ohm, *supra* note 16, at 1140.

250. *See, e.g.*, Richard A. Hertling & Kaitlyn McClure, *In Congress: Trade, Privacy, Fiscal Year 2017*, LAW360 (Apr. 24, 2016), http://www.law360.com/articles/788308/in-congress-trade-privacy-fiscal-year-2017; *Republican/Conservative Bills Supported and Opposed*, MAPLIGHT (Jan. 25, 2017), http://maplight.org/us-congress/interest/J1100/bills.

251. *See, e.g.*, Thorin Klosowksi, *Lots of Health Apps Sell Your Data. Here's Why*, LIFEHACKER (May 9, 2014, 10:00 AM), http://lifehacker.com/lots-of-health-apps-are-selling-your-data-heres-why-1574001899.

1. Peer Data Purchase as Privacy Intrusion

The Second Restatement of Torts defines the tort of intrusion upon seclusion as follows: "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be *highly offensive* to a reasonable person."[252] The Restatement's Comments clarify that the intrusion may involve some form of investigation or examination into a person's private concerns, "as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by forged court order to permit an inspection of his personal documents."[253] Thus, it is possible that courts could view the purchase of a peer's sensitive data—such as their emails or GPS data—as an investigation that intrudes on their seclusion.

Courts to date have held that the sort of incursions upon privacy that result from data sale fall well short of the "highly offensive" standard.[254] Relational control poses two new dilemmas for common law courts to consider in the years ahead. First, as a preliminary matter, whether a plaintiff can claim a privacy interest in the data that are legally controlled by a third party. Second, whether an acquaintance's purchase of the plaintiff's data is highly offensive to a reasonable person.

It is a structural feature of the digital age that one's personal data, over which it was once possible to exercise sole control, are now inevitably possessed by some third parties.[255] Whatever one does online will be recorded by many entities—among them the commercial ISPs, third party advertisers, host websites (as well as perhaps an array of state intelligence agencies). Internet users should not lose their privacy interests in their most intimate data simply because the structure of the internet does not allow them to operate online without some actors gaining control over the records of their online activity.[256] This view is supported by Justice Sotomayor's concurrence in *U.S.*

252. RESTATEMENT (SECOND) OF TORTS § 652B (Am. Law Inst. 1977) (emphasis added).

253. *Id*. cmt b.

254. *See supra* Section II.B.

255. *Cf*. Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J.F. 8, 15 (Apr. 27, 2016) ("To this extent, I agree with those who criticize the broad proposition that *any* information that is disclosed to third parties is outside the protection of the Fourth Amendment. Courts can appropriately take into account whether information is content or non-content information, whether it is publicly disclosed through social media or is stored in the equivalent of the cloud, or whether its exposure is 'voluntary' only in the most technical sense because of the demands of modern technology." (emphasis in original))

256. *See* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions ("91% of adults in the survey 'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies."). Even the technologies that allow "anonymous browsing" should probably not be viewed as reliably private, as intelligence and both

v. Jones, which pushed back on the idea that third party possession of data invalidates an expectation of privacy from other third parties.[257] As a threshold issue to determine whether certain instances of relational control may constitute a tortious invasion of privacy, courts should recognize a continued privacy interest in private information that necessarily must exist in the hands of certain third parties.

In order to recognize an intrusion tort for certain instances of relational control, courts would need to find that the intruder's purchase of data was "highly offensive." Some courts have interpreted the "highly offensive" standard as an unreasonably high bar to recognizing intrusion case. For example, some courts have held that an individual's unauthorized access of another's email failed to meet the standard for "highly offensive" behavior,[258] an interpretation that seems unreasonable given that the Second Restatement's comment includes the opening of mail as an example of intrusion. Similarly, it would seem that a consumer's purchase of another's GPS data or bank transactions could constitute an intrusion upon that person's seclusion.

A legal prohibition that target's the purchaser's behavior nevertheless also invites pitfalls. An overbroad interpretation of "highly offensive" could undermine the value of consumer data that is sold to commercial entities for advertising purposes. Similarly, an expanded intrusion tort could chill digital consumers' acquisition of consumer information for non-harmful ends. As courts consider the specific fact patterns that would trigger liability for intrusion, courts should understand "highly offensive" in light of evolving norms of digital activity, while being careful not to invite over enforcement with too broad a construction.[259]

government and commercial entities will remain in a tug of war over activity that takes place over these technologies.

257. *See* 565 U.S. 400, 418 (Sotomayor, J., concurring) ("But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."). *See also id*. at 427-29 (Alito, J., concurring) (observing that privacy expectations are in flux in the new technological environment that allows wireless carriers to store precise GPS data, and arguing that legislatures are better suited than courts are to address privacy standards).

258. *See, e.g*., Smyth v. Pillsbury Co., 914 F. Supp. 97, 11 I.E.R. Cas. (BNA) 585, 131 Lab. Cas. (CCH) ¶ 58104 (E.D. Pa. 1996) (applying Pennsylvania law, holding that despite assurances that e-mail communications would not be intercepted, management's confiscation of an employee's email was not highly offensive because the emails sent included inappropriate and unprofessional comments); Thompson v. Ross, 2010 WL 3896533 (W.D. Pa. 2010) (applying Pennsylvania state common law, dismissing plaintiff's claim that his ex-girlfriend had provided his personal computer to coworkers, who were able to gain, search, and extract old emails from the computer hard drive, because he failed to show that his employer invaded his privacy).

259. For example, it might be unwise to expand intrusion doctrine such that it covers behavior like the hypothetical that opened this Note, as it is increasingly common practice to research a new person before you meet them. *Cf*. Maureen O'Connor, *The New Abstinence: Not Googling Your Date*, NYMAG (June 22, 2014), http://nymag.com/thecut/2014/06/new-abstinence-not-googling-your-date.html.

2. Unrestrained Data Sale as Negligent

While an expanded intrusion tort could allow certain victims of relational control to sue their controller, common law courts could also expand negligence doctrine to allow suit against the data seller, taking the route of chopping at supply rather than demand. As noted, courts to date have been leery to find data brokers negligent in the data sale context.[260] However, given the permanence of data and the breadth of its subsequent uses, courts should consider whether sales of highly sensitive data (in type or scope)—particularly with no contractual restrictions on subsequent use or sale—place consumers at unreasonable risk.

C. Balkin and Ohm Frameworks as Ex Post Protections

As discussed in Part V, Balkin and Ohm each advance proposals that could protect consumers from this new avenue for digital abuse, while still accommodating a digital environment that places highly sensitive information in the hands of a diverse array of commercial entities.

Ohm's proposal should be expanded in federal and state regulations to construe a far wider category of information as sensitive. U.S. laws governing sensitive data should recognize not only communications metadata, but also new data types—including calendar data, browsing history, social network data, purchase records, and other information that could provide insights into a person's personality and habits. Expanding the data types that U.S. law recognizes as sensitive would trigger various regulatory protections—including the FIPPs of "purpose specification" and "use limitation"—for data that could be particularly harmful in the context of relational control.[261]

This recommendation could prove costly, as expanding the types of data that regulators consider sensitive would likely increase the proportion of companies that need to submit to burdensome regulatory safeguards. Over-protective regulations could also curb the development of many important, pro-societal benefits that stem from the efficient commercial access to consumer data.[262]

Balkin's conception of information fiduciaries should be construed to require companies to limit the risk of privacy harms that stem from secondary use. The framework should support regulations that could, for example, require companies to encrypt data while in storage and allow data sale only in the context of contractual rules that forbid re-identification and subsequent,

260. *See supra* Section II.B.

261. Ohm, *supra* note 16, at 1138.

262. This Note has not extensively explored the benefits of our current data broker regime. *See, e.g.*, Ohlhausen & Okuliar, *supra* note 16, at 121-24 (describing a broad array of consumer and societal benefits advanced by data availability in the United States). These benefits require careful weighing of the regulatory intervention.

purpose-flexible resale. Such duties would limit brokers' access to consumer data, but also likely impose transactional costs.[263]

D. Privacy Opt-ins for Data Sale

Privacy policies remain a particularly fertile ground for privacy reform. The FTC's Section 5 enforcement actions take aim at companies that lack privacy policies and at those whose behavior deviates from their stated policies.[264] As Solove and others have noted, opt-outs are common provisions in privacy policies, often requiring a consumer to check a box, call, or mail the company within a certain time period to confirm their choice.[265] However, opt-outs also come with risks, including a consumer's implied, unwitting consent to policies that may prove detrimental.[266] In order to avoid setting consumers up for bad "deals," the FTC should explore requiring companies to include a narrow set of clear, logistically smooth opt-in provisions regarding the sale of collected data. Requiring that companies receive from consumer consent that was not tied to a reduction or denial of service would provide a strong mechanism for consumers to protect themselves against the threat of relational control.

These proposed changes to privacy doctrine will not inoculate consumers from the threat of relational control, nor are they immune to criticism. However, in tandem or in isolation, these proposed shifts to U.S. privacy law will help manage a problem, which, unconstrained, may only grow in extent and intensity.

Conclusion

Under the current legal regime, a person's intimate information can be acquired by someone in his or her social or professional circles for the purpose of exercising control. This threat is growing and adds to the imperative that digital privacy be properly protected. Although a decisive solution to this problem may prove elusive, there are a handful of doctrinal reforms that, if implemented, will significantly reduce consumer exposure to relational control.

The relational control problem also underscores the oft-overlooked *contextual* features of digital privacy. As society has moved from the analog to the digital age, individuals have lost the ability to exercise sole control over their private information. The records of digital activity are controlled by many

263. *See also* Sebastian Zimmeck, *The Information Privacy Law of Web Applications and Cloud Computing*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 451 (2013).

264. *See, e.g.*, Solove & Hartzog, *supra* note 102, at 598.

265. *See, e.g.*, DANIEL J. SOLOVE & PAUL M. SCHWARTS, INFORMATION PRIVACY LAW 828-35 (5th ed., 2015); Sovern, *supra* note 177.

266. Solove, *supra* note 16 (critiquing "privacy self-management" as failing to provide people with meaningful control over their data).

actors, from private ISPs to state intelligence services, which exist beyond a consumer's ability to meaningfully influence them.

Privacy violations that lead to relational control are inherently context dependent. The data that might be harmless in the hands of an entity like Facebook or a federal agency can be dangerous if possessed by a professional or social rival. Any legal intervention that aims to protect consumers from relational control must recognize this contextual feature of privacy—that what is important is not only *what* others may know but also *who* may know it.