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

Theodore Rostow

[THIS DOCUMENT IS A DRAFT OF A FORTHCOMING NOTE THAT WILL APPEAR IN THE 34TH VOLUME OF THE YALE JOURNAL ON REGULATION. THIS DOCUMENT MAY BE USED FOR TESTING LEGAL-CITATOR, AND MAY BE DISSEMINATED IN CURRENT FORM WITH ATTRIBUTION. WHEN PUBLISHED, THE AUTHOR (THEODORE ROSTOW) AND THE YALE JOURNAL ON REGULATION WILL JOINTLY HOLD COPYRIGHTS WITH ADDITIONAL TERMS AND CONDITIONS THAT APPLY TO THE PUBLISHED DOCUMENT.]

*Privacy scholarship to date has failed to consider a new development in the commercial privacy landscape. Data brokers have begun to sell data products to individual consumers interested in tracking the activities of love interests, professional contacts, and other people of interest. This practice creates an avenue for a new type of privacy harm—“insider control”—which privacy scholarship has yet to recognize.*

*U.S. privacy laws fail to protect consumers from the possibility of insider control. Apart from two noteworthy frameworks that might offer paths forward, none of the viable reforms offered by privacy scholars would meaningfully limit consumers’ vulnerability. This Note proposes changes to existing privacy doctrines in order to reduce consumers’ exposure to this new harm.*

Introduction: 2

A New Privacy Harm: 5

Part I: U.S. Commercial Privacy Law 10

A. Statutory Privacy Protections in the Commercial Sphere 10

B. Court Limitations on Privacy Protection 13

C. Agency Regulation of Data Transactions 15

Part II: The Data Broker Industry and the Market for Buying People’s Data 18

A. The Booming Broker Industry 18

B. Data Sales to Individual Consumers: 19

Part III: Data Sale as a Weaponization and the Threat of Insider Control 20

The Coming Emergence of Insider Control: 23

Part IV: Proposed Reforms Fail to Remedy Insider Control 29

Broker-facing Reforms: 29

Reforms for Information Services: 32

Privacy-enhancing Consumer Technologies: 35

Part V: “Information Fiduciaries” and “Sensitive Data”: Promises and Limits 36

Sensitive Data and Insider Control: The Beginnings of a Solution? 37

Information Fiduciaries and Insider Control: A Second Path Forward? 40

Part VI: Doctrinal Shifts in Light of Insider Control 43

Congressional Privacy Reforms: 44

Privacy Intrusion Reconsidered: 45

Balkin and Ohm Frameworks as ex post Protections: 48

Privacy Opt-ins for Data Sale: 50

Conclusion: 51

# 

# **Introduction:**

The information that companies possess about U.S. consumers has expanded to an unprecedented extent in the past two decades. Data on what people watch, buy, eat, say, think, and feel are available for sale.[[1]](#footnote-1) Everyone with access to the web produces salable personal data, and an array of private and public entities are collecting, storing, and trading such personal data. Data sales occur in a space particularly removed from oversight or regulation, posing novel, unconsidered threats to consumers.

\*\*\*

Imagine, for a second, 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 seem like an excellent fit. You share many common interests—from favorite television shows to the websites you read every morning.  They share your political sensibilities and your concerns about the future. You recommend them enthusiastically for the position, and they are hired on your recommendation.  Unfortunately, you learn that the candidate, when they arrive on the job, has none of these attributes.  They simply paid $2.45 to buy data on what shows you watched and articles you read.

Or, instead, imagine that you meet someone on OkCupid for a date. While you are usually cautious around complete strangers, you have many overlapping interests and have spent time oversees in similar places, so you decide to throw caution to the wind and meet for dinner. You have a wonderful time talking about a number of mutual friends you knew from childhood but with whom you have since lost touch. You invite the person back to your place for the night. When you wake up the next morning, you find that your house has been ransacked and your phone, laptop, and wallet are gone. The date had spent $0.35 for your Facebook friend list and basic profile information, and another $1.65 for the history of your recent browser history and travel purchases.

\*\*\*

We live in a world where the events described above can and increasingly will occur. There is a growing market and demand for personal data and the data broker industry has expanded considerably over recent years. Currently, 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”[[2]](#footnote-2) —purchase, compile, and sell personal data to an array of actors. While relatively little is known about the virtually unregulated and notoriously opaque data broker industry, what is known creates concern.

In 2014, the Federal Trade Commission (FTC) published a study of the commercial practices of nine data brokers and documented the extent of the data that have been collected on consumers. Acxiom, one of the largest data brokers, acknowledges that it has an average of over 3,000 pieces of data on every U.S. consumer.[[3]](#footnote-3) Datalogix, a broker that provides data to business on the spending of nearly every U.S. household, has collected data on more than one trillion dollars in consumer spending.[[4]](#footnote-4) In the aftermath of the FTC report, several journalists have explored the size[[5]](#footnote-5) of this self-regulated[[6]](#footnote-6) industry, and the price for which data are sold.[[7]](#footnote-7)

These reports reveal that, while most brokers generate profits by selling data to commercial entities, brokers have begun to generate significant revenue also by selling consumer data *to other consumers*.[[8]](#footnote-8) The nine firms the FTC studied in 2014 generated more than $52 million in annual revenue by selling products intended primarily for individual consumers, who may 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.”[[9]](#footnote-9) This consumer-focused practice will likely grow over the next few years.

While a growing number of privacy scholars have written on the data broker industry,[[10]](#footnote-10) this Note is the first to consider the implications of an unregulated data market that allows individuals to purchase information about others without their knowledge or consent.

# 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?[[11]](#footnote-11) Courts require plaintiffs to show a tangible, financial harm before they will recognize a privacy violation.[[12]](#footnote-12) This legal requirement has led privacy scholars to devote considerable energy to identifying (or dismissing)[[13]](#footnote-13) the harms that a lack of privacy can impose.[[14]](#footnote-14) For example, Daniel Solove sought to map all privacy harms that can be connected to digital activity.[[15]](#footnote-15) Recent scholarship builds on his efforts, especially with respect to the evolution of privacy violations into direct or indirect discrimination.[[16]](#footnote-16) In a recent article surveying the history of privacy regulation in the United States, Maureen Ohlhausen and Alexander Okuliar concludes 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.[[17]](#footnote-17)

Scholars have mapped privacy harms that flow from the collection,[[18]](#footnote-18) aggregation,[[19]](#footnote-19) use,[[20]](#footnote-20) and dissemination[[21]](#footnote-21) of digital information.[[22]](#footnote-22) These harms range[[23]](#footnote-23) from the less tangibly harmful—including ill ease or anxiety[[24]](#footnote-24) at the prospect of being constantly monitored (which can also lead to self-censorship[[25]](#footnote-25)), consumer manipulation by companies,[[26]](#footnote-26) and voter manipulation by campaigns[[27]](#footnote-27)—to the more tangible harms, such as blackmail[[28]](#footnote-28) and stalking.[[29]](#footnote-29) Identified harms also manifest in social sorting and discrimination,[[30]](#footnote-30) an increased vulnerability to cyber attacks,[[31]](#footnote-31) and identity theft.[[32]](#footnote-32)

Scholarship on data sale, both in general[[33]](#footnote-33) and relating to the data broker industry in particular,[[34]](#footnote-34) relies on the harms that scholars like Daniel Solove and others have identified. David Vladeck’s recent analysis of the effect of data brokers on commercial privacy highlights three privacy harms—identity theft (the most urgent) and data breaches, and the unrestrained collection of sensitive, personal data.[[35]](#footnote-35) Rebecca Lipman underscores both how data brokers provide capacity for third parties to deliver targeted advertising,[[36]](#footnote-36) as well as how these datasets, which often contain inaccurate information that consumers do not know about and often cannot correct, can facilitate harmful social sorting.[[37]](#footnote-37) Amy Schmitz argues that data sale can foster discrimination and augment preexisting power imbalances through secret scoring and segmenting of consumers’ economic value.[[38]](#footnote-38) These are important concerns that are implicated by the growth of this opaque, rapidly growing industry. However, they also mirror those raised by existing privacy scholarship and do not contemplate distinct, new harms that may stem from data sale.

This Note breaks from these scholars’ perspective on data sale and brokers by arguing that the creation of a market for individuals to buy data on their peers enables a new privacy harm: “insider control.” The hypotheticals described above are an example of this new privacy harm. Insider control occurs when individuals use the private, covertly acquired data of those in their social or professional networks. When data brokers sell data to individuals, they allow individuals to acquire informational advantages by purchasing a wide array of data that allow important, context-dependent insights. These insights allow individuals to exert meaningful influence or even control over 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 existing U.S. law in the commercial realm and how the existing laws fail to provide remedies for most insider control harms. Part II surveys the data broker industry and the market for data that is sold to individuals. Part III outlines some possible implications for insider control and why we should expect threat of insider to grow.

Part IV assesses the prominent legal interventions that scholars have proposed to the commercial privacy problem and explains why prominent reforms that target data brokers’, online companies’, and consumers’ data practices all fail to remedy consumers’ vulnerability to insider control. Part V explains why two recent proposals—Jack Balkin’s “information fiduciaries” framework and Paul Ohm’s “sensitive information” approach—offer possible approaches for reducing the likelihood of insider control, even as each framework as presently constituted would fail to protect consumers against the threat. Part VI proposes, and highlights the possible shortcomings of, a set of multi-tiered, ex ante and ex post, doctrinal shifts in existing privacy law that may reduce consumer exposure to the threat of insider control.

# **Part I: U.S. Commercial Privacy Law**

# A. Statutory Privacy Protections in the Commercial Sphere

The United States has adopted a patchwork, sectoral approach to privacy law in the commercial sphere.[[39]](#footnote-39) The Fair Credit Reporting Act (FCRA) imposes an array of obligations on consumer reporting agencies and offers protections for our credit information.[[40]](#footnote-40) For example, the FCRA grants individuals the right to request a copy of their credit report, limits the freedom to share credit reporting, and obligates agencies to correct errant information.[[41]](#footnote-41) The Family Educational Rights and Privacy Act (FERPA) protects students’ educational records.[[42]](#footnote-42) The Health Information Portability and Accountability Act (HIPAA) governs how doctors and medical services must protect the data of their patients,[[43]](#footnote-43) while the Gramm-Leach Bliley Act (GLBA) regulates the activity of the financial industry and imposes privacy requirements for data about financial transactions.[[44]](#footnote-44) A particularly important piece of legislation to this inquiry is the Stored Communications Act (SCA).[[45]](#footnote-45) The SCA, along with the Wiretap Act, regulates government’s access to digital communications. In the commercial sphere, the SCA limits the ability of commercial internet service providers (ISPs) to reveal certain content to nongovernmental entities.[[46]](#footnote-46)

We should not overstate the adequacy of these statutory protections, and many scholars have questioned their fundamental efficacy.[[47]](#footnote-47) 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.[[48]](#footnote-48) 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.[[49]](#footnote-49) Similarly, FERPA does not impose rules on the data that school support applications collect, which allow companies to make “consequential inferences” about “a child’s intelligence or interests.”[[50]](#footnote-50) Paul Ohm notes how the GLBA only applies to a narrow subset of entities that are defined by the statute as a “financial institution.”[[51]](#footnote-51) 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.[[52]](#footnote-52)

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 (deeply flawed)[[53]](#footnote-53) SCA and (far more robust) Children’s Online Privacy Act (COPPA).[[54]](#footnote-54) Despite describing an outdated and arcane technical reality, courts have interpreted the SCA to protect certain communications (such as text messaging) that many applications cannot sell to brokers.[[55]](#footnote-55) The SCA, however, does not extend to wall posting or comments, and its language—passed in 1986 as part of the Electronic Communications Privacy Act—that distinguishes these services does not cohere in today’s technological environment.[[56]](#footnote-56) 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,”[[57]](#footnote-57) and the FTC has made clear that this definition expands as technology changes to cover mobile apps, plug ins, and third party networks.[[58]](#footnote-58) These narrow exceptions notwithstanding, Congress has passed no statute that imposes meaningful checks on data broker activity.

State legislation similarly provides few checks on broker activity. While California has moved to expand privacy protections more than any other state, these regulations generally do not affect data brokers. Of note, California has passed legislation that (1) expands the SCA to prohibit employers from looking at the private social networks of employees and prospective employees (which does not affect brokers),[[59]](#footnote-59) (2) requires businesses that collect personally identifiable information to prominently list their privacy policy (which does),[[60]](#footnote-60) and (3) requires companies to disclose what information they share to companies for marketing purposes (which does not).[[61]](#footnote-61) Additionally, scholars note how, outside of California, most state legislation has focused on data security, rather than privacy.[[62]](#footnote-62)

# B. Court Limitations on Privacy Protection

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.[[63]](#footnote-63) Local control concerns are most directly implicated by intrusion, which the Second Restatement of Torts defines 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.”[[64]](#footnote-64)

In addition to showing that a data transaction constituted an intrusion upon their seclusion (or, because of the particular actors, satisfied a statutory hook, like the FCRA), a prospective plaintiff must also show how the transaction or subsequent use of the purchased data satisfies Article III standing requirements. To show standing, a plaintiff must demonstrate that an injury-in-fact occurred by showing a harm that is both concrete and particularized.[[65]](#footnote-65) These twin standing and tort requirements have led courts to reject a number of privacy claims that challenge the sale of information.

In *Shibley v. Time, Inc.,* an Ohio court dismissed a plaintiffs’ suit against magazine publishers that sold subscription requests to direct mail advertisers.[[66]](#footnote-66) The court held that although the purchasers of the lists could learn about the plaintiff’s lifestyle, the sale of lists did not “cause mental suffering, shame or humiliation to a person of ordinary sensibilities.”[[67]](#footnote-67) 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 based on their spending habits.[[68]](#footnote-68) 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 grizzly murder, left the door ajar that a data broker might be liable under negligence, where criminal activity could have been predicted. In *Remsburg v. Docusearch, Inc.*,[[69]](#footnote-69) a New Hampshire resident purchased an acquaintance’s personal information from an information broker in order to stalk and ultimately murdered her. Due to the particular targeted nature of the New Hampshire resident’s inquiries,[[70]](#footnote-70) the court found that an early data broker might be liable for negligence if the buyer’s manifest activity suggested foreseeable criminal misconduct against the target of their 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,”[[71]](#footnote-71) and, 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 court remedies, federal agencies have proved more responsive to digital privacy concerns. Of particular significance is the action by the Federal Communications Commission (FCC) to impose a number of new regulations on internet service providers (ISPs).[[72]](#footnote-72) Recognizing that “there are currently no rules in place outlining how ISPs may use and share their customers’ personal information,”[[73]](#footnote-73) the FCC voted 3-2 to require ISPs to disclose they types of information they collect, the purposes for which the data are used, and what information they share.[[74]](#footnote-74)

While it remains uncertain how these rules will affect ISP data sale, the rules add increase transparency and add a barrier between brokers and one source of certain sensitive information.[[75]](#footnote-75)

Outside of ISP regulation,[[76]](#footnote-76) the FTC has been the leading advocate for consumer privacy, issuing over 170 privacy complaints against companies for privacy violations.[[77]](#footnote-77) The FTC derives its authority from § 5 of the Federal Trade Commission Act to prohibit “unfair or deceptive acts or practices.”[[78]](#footnote-78) 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, despite the company’s promise that the messages would disappear, they were stored on Snapchat servers.[[79]](#footnote-79) As part of the consent decree, Snapchat agreed to submit to 20 years of monitoring to ensure it did not deceive customers.[[80]](#footnote-80) The FTC has entered into similar consent decrees with Facebook, when in its early days it did not adhere to its privacy policies,[[81]](#footnote-81) and other apps whose privacy policies are deceptive (as opposed to merely vague and lawyerly, as is the norm).[[82]](#footnote-82)

On narrow occasions, the FTC has also moved against data brokers. In 2006, a data broker was ordered to pay civil penalties after the FTC alleged that a consumer data broker violated the FCRA by furnishing credit reports to subscribers.[[83]](#footnote-83) 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.”[[84]](#footnote-84)

These actions constitute two narrow exceptions to the general rule of FTC non-intervention, as the FTC may only pursue action against (1) commercial activity that violates existing law, or (2) activity that involves the broker knowingly facilitating crimes.[[85]](#footnote-85) 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.[[86]](#footnote-86) Unless data brokers violated the (incredibly vague) privacy policies they usually have, the FTC would not have the authority or justification to allege unfair business practices or any other statutory violation if data brokers en mass began to sell consumer data to other consumers.

# **Part II: The Data Broker Industry and the Market for Buying People’s Data**

In the absence of legal regulation, the data broker industry has expanded considerably over the past few years. Despite its expansion, little is known about the broker industry,

# A. The Booming Broker Industry

A *Newsweek* report estimates that the data broker industry involves between 2,500 and 4,000 data brokers.[[87]](#footnote-87) Unlike large companies like Google and Facebook, data brokers try to avoid name recognition,[[88]](#footnote-88) while collecting data on American consumers.[[89]](#footnote-89)

Brokers collect information from a wide array of sources. Major sources of data are federal and state governments, which provide information, including about recreational and professional licenses, bankruptcies, driving histories, voter registration, mortgages, birth, marriage, divorce, and death records.[[90]](#footnote-90) Data brokers scrape publicly available data from sites like LinkedIn and other public information from social media sites and blogs.[[91]](#footnote-91) Of the nine data brokers surveyed, eight bought data from commercial entities, including purchase information (including dates of transactions, dollar amounts spent, types of card used), aggregated transactional data from financial services companies.[[92]](#footnote-92) At least one of the nine brokers purchases consumers’ web browsing activities from online advertising networks.[[93]](#footnote-93) As many commentators note, there is no legal regime that prevents brokers and other companies from sharing data to individuals and companies,[[94]](#footnote-94) and a wide array of entities—from political campaigns[[95]](#footnote-95) to antivirus companies[[96]](#footnote-96)—buy and sell data with brokers.[[97]](#footnote-97)

# B. Data Sales to Individual Consumers:

The big data market is lucrative. The nine brokers surveyed by the FTC generated a combined $426 million in annual revenue. In general, this revenue stems from three types of revenue: marketing, risk mitigation, and “people search.”[[98]](#footnote-98) Most relevant to this Note’s inquiry is people search, as this collection of services that comprise people search is “often intended for use by individuals.”[[99]](#footnote-99) The FTC noted how “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.”[[100]](#footnote-100) Among the nine firms, people search services generated $52.69 million in annual revenue. The FTC report’s finding on people search shows that there are already products offering data on other people to individuals in their social and professional networks. Thus, the FTC report provides conclusive evidence that data brokers have begun to sell data about consumers to consumers.

As described, few laws limit the sale of information to consumers. Brokers occasionally include restrictions in contracts of sale so that they do not run afoul of the FCRA, GLBA, HIPAA, or COPPA.[[101]](#footnote-101) 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.”[[102]](#footnote-102) Statutes do not require more than these protections, which buyers or sellers impose *ad hoc*.[[103]](#footnote-103)

# **Part III: Data Sale as a Weaponization and the Threat of Insider Control**

Insider control rests on two assumptions. First, informational advantages are incredibly powerful in “insider” relationships.[[104]](#footnote-104) By “insider,” I refer to people who are part of the same network: peers and co-workers, supervisors and subordinates, friends and romantic interests, as well as acquaintances and friends of friends. Privacy scholarship as a general matter does not consider “insider relations” as the context in which privacy harms may take place. One exception, however, is privacy threat scholar Felix Wu,[[105]](#footnote-105) who briefly the possibility of privacy invasions by insiders in the context of data releases.[[106]](#footnote-106) Wu defines “privacy ‘insiders’ [as] those relationship to a particular individual allows them to know significantly more about that individual than the general public does.”[[107]](#footnote-107) Wu notes that harms from 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.”[[108]](#footnote-108) Privacy insiders may interact with each other in the physical world with varying degrees of closeness and trust. Informational asymmetries between these relationships have a distortive effect on these relationships’ natural course.[[109]](#footnote-109) When armed with an informational edge over another in one’s network, an individual has the capacity to nudge, manipulate, and, ultimately, exert control over that person and their related networks.[[110]](#footnote-110)

Second, the availability of information for sale allows individuals to acquire the data of others in their networks. As discussed, the data broker industry is wholly self-regulated and only at times operates according to a set of voluntary guidelines that have been adopted by the internet and advertising industries.[[111]](#footnote-111) The diversity and number of actors in the broker industry creates the possibility that a person’s internet activity may wind up in the hands of *any* buyer. The FTC study on data brokers demonstrates that these data transactions already occur to the tune of $52 million.[[112]](#footnote-112) As the FTC observed, motivations for individual consumers to purchase data include to “track[] the activities of executives and competitors,” to “research[] a potential love interest or neighbor,” or to “network[].”[[113]](#footnote-113) Little yet is known about the individuals that purchase others’ data or their motivations. However, we do know that this activity is legal and occurs with no oversight.

We should understand the current data sale environment as a weaponization. The data sale environment creates a diverse array of unregulated platforms that can convey data collected anywhere into the hands of any interested person who is well positioned to use this informational advantage to benefit themselves and harm others. There seems to be no way to protect consumers in this environment absent new laws, the effectiveness of which, if implemented, remains unclear.

# The Coming Emergence of Insider Control:

In addition, we should expect the market for peer data to grow, perhaps dramatically. Five factors suggest that the incipient market for peer data will increase over the next few years, which should raise significant concerns for privacy scholars, lawmakers, and consumers.

*Factor 1: People have a lot to gain from the purchase of others’ data.*

Information drives human society and is at the heart of every human decision. There is a reason why intelligence gathering has been a central tool of statecraft since time immemorial. Even outside of the national security realm, however, all human decisions and actions are based on a wide array of indiscernible factors and variables. The commoditization of data provides a lens with which to view these determinants of human behavior.

With data, one can know what causes a person to feel joyful or stressed, what people read or watch for information, levity, or stress-release. Data provide a map of one’s social interactions—conversations, rivalries, romantic interests, and bitter pasts. Data captures compulsions, neuroses, and lusts. It helps reveal personality flaws and strengths. Biometric data provides even more nuance: as it 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.[[114]](#footnote-114)

Why is this important? Because deeply personal insights can be derived from this information and, with it, an unprecedented ability to exert control over peers and acquaintances.[[115]](#footnote-115) The opening hypotheticals show two examples when an asymmetric access to information on others can change the trajectory of conversations, affect what people think and feel, and influence targets’ decisions about who to date or hire. These are far from the only examples, as gaining access to information can provide insights that can inform strategic decisions from boardrooms to bedrooms, and everywhere in between. In short, data are powerful, and individuals, like corporations or states, have much to gain from acquiring information on those around them. That data edges can provide clear social, professional, romantic, and political benefits is a key reason we should expect the problem of insider control to grow significantly over the near term.

*Factor 2: Information is incredibly cheap.*

Hand in hand with the theoretical observation that people have much to gain from buying data on those around them is the practical observation that data are shockingly cheap. The *Financial Times* has published a series of articles on the burgeoning market place for consumer data.[[116]](#footnote-116) While data brokers make tens of millions of dollars in annual revenues, the cost of buying personal data is astonishingly cheap. Basic information about a person’s age, gender, and location is worth a mere $0.0005 per person.[[117]](#footnote-117) More targeted commercial information—that someone is looking to purchase a car or a vacation—is only marginally more expensive: $0.0021 a person.[[118]](#footnote-118) Marketers will pay $0.11 to know that a woman is pregnant and in her second trimester.[[119]](#footnote-119) While the cost of data increases with the intimacy of the information, the prices per person remains low—$.26 per person will buy access to lists of people with specific health conditions or taking certain prescriptions.[[120]](#footnote-120) 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.[[121]](#footnote-121)

*Factor 3: No rules proscribe individual data purchases.*

As noted in Part I, there are no robust obstacles to individuals buying data on most people’s online activities.[[122]](#footnote-122) The sector-by-sector approach that the United States has taken to privacy regulation leaves few general rules governing what, in general, people may do with data.[[123]](#footnote-123) The FTC itself acknowledges that no laws or regulations exist to restrict what data may be bought and sold.

*Factor 4: No easy legal fixes can ameliorate this threat.*

The legal context informing this Note is unlikely to change soon. Not only is the general approach of U.S. law towards commercial privacy unlikely to change, but data sale is an enormous, multi-billion dollar industry that also provides many positive benefits—from greater efficiency to the delivery of tailored services. There is no obvious panacea to the insider control problem that would not significantly change how the U.S. regulates entire industries. Part of the reason for this challenge is the subtle nature of the threat posed by insider control. At its most benign (yet still troubling) insider control is simply the purchase and use of commercially traded information to gain insight into how one should act.

Further, constitutional roadblocks would likely deter many possible interventions, as First Amendment scholars underscore that data sale likely constitutes protected speech.[[124]](#footnote-124) While this Note proposes a number of regulatory, tort, statutory, and private law reforms that help mitigate the threat of insider control, these are by no means simple or cure-all fixes.

*Factor 5: Anonymization is a frail tool, and perhaps irredeemably so.*

Finally, we should expect the problem of insider control to spread because of the well-documented problem of data anonymization. The common response to consumer privacy concerns of many commercial entities is to remove all identifying features from a data set.[[125]](#footnote-125) The use of anonymization techniques is pervasive in data transactions. For example, HIPAA requires that health data be anonymized,[[126]](#footnote-126) and creates a safe harbor for companies that removed from datasets 18 types of identifiers (including, for examples, names, addresses, IP addresses, and social security numbers) and also had “[n]o actual knowledge [that] residual data can identify individual[s].”[[127]](#footnote-127) Similarly, a vast number of companies, including banks,[[128]](#footnote-128) credit cards companies,[[129]](#footnote-129) anti-virus software,[[130]](#footnote-130) telecommunications companies,[[131]](#footnote-131) ISPs,[[132]](#footnote-132) internet companies,[[133]](#footnote-133) and data brokers themselves sell anonymized, de-identified data to other companies.[[134]](#footnote-134)

The problem, however, as many computer scientists, data analysts, and privacy scholars have shown, is that this is an ineffective tool.[[135]](#footnote-135) Surveys of common anonymization and de-anonymization methods reveal the ease with which computers and humans can re-identify anonymized datasets. For both explicit (intentional, such as the sale of anonymized and sanitized datasets) and implicit (unintentional, such anonymized data or partial datasets that are often released after major hacks as hacked data),[[136]](#footnote-136) a number of de-anonymization attacks powerfully and efficiently re-identify anonymized datasets. The most effective attack, and most relevant for our inquiry, involves the attacker leveraging auxiliary information or background knowledge to identify the matching dataset.[[137]](#footnote-137) An example of this type of attack was conducted on the Netflix Prize dataset. 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.[[138]](#footnote-138) 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.”[[139]](#footnote-139)

Sarah Jamie Lewis also provides a vivid demonstration of how easily identities can be exposed in anonymized datasets. She surveyed how a 20GB dataset, comprising more than 173 million individual taxi trips with anonymized licenses, medallion numbers, and other metadata could easily be subsequently re-identified.[[140]](#footnote-140)

Data, even when scrubbed, are easy to connect to regions or demographic groups. This feature of datasets is why they are valuable. Companies, governments, and individuals purchase datasets because they seek to gain insights about real people’s behavior. Accordingly, it seems unlikely that a technical solution will emerge to the de-anonymization problem that would not jeopardize the fundamental reason that data is valuable.

These factors suggest that the consumers will buy more data on their peers in the years ahead. Consumers do not consider this possibility when they use the internet or read third party sharing disclosures on company privacy policies. The existence of insider control, which can facilitate significant manipulation in almost any human venture, requires a robust policy response that can protect consumers from this new privacy harm.

# **Part IV: Proposed Reforms Fail to Remedy Insider Control**

Part III examines how privacy scholars have proposed to solve harms related to the sale of digital information. As insider control has not been discussed in scholarship, it should not surprise that no proposals effectively address this vulnerability.

# Broker-facing Reforms:

When it released its 2014 Report, the FTC 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) then empower consumers to dispute the accuracy of data collected, which brokers would then have to investigate and correct erroneous information.[[141]](#footnote-141) The FTC also expanded upon the DATA proposals in several ways. First, the FTC proposed creating a central website that listed the largest fifty data brokers and linked to their access tools and opt-out policies.[[142]](#footnote-142) Second, the FTC proposed legislation that would require brokers to disclose who brokers sold data to and notify customers when collected data adversely affected a consumer transaction.[[143]](#footnote-143) Third, and perhaps most promising, while not requiring individuals explicit consent for brokers to sell data, the FTC proposed legislation that would require consumers to *opt-in* to sharing of any sensitive data, such as “certain health data.”[[144]](#footnote-144)

A number of privacy scholars have proposed additional reforms in light of the FTC data broker report. These range from the advocating legislation in line with the EU’s Data Privacy directive[[145]](#footnote-145) to expanded disclosure and correction requirements.[[146]](#footnote-146) 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.[[147]](#footnote-147)

However, these proposals, as well as those made by the FTC, would fail to address the problem of insider control. The goals of these proposals are to limit harms that have been tied to the practices of data brokers—for example, discrimination or the denial of opportunities based on incorrect information. A recent empirical study of consumer reactions to privacy disclosures notes that these proposals rely on “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.”[[148]](#footnote-148) However, the novel proposals articulated by this study—which include 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 insider control.[[149]](#footnote-149)

These proposals fail because they have not considered the possible distinct harms that could result from individuals buying data on their peers’ activity. Accordingly, these proposals would not prevent individuals from purchasing data to manipulate the decisions of peers, rivals, romantic interests, or colleagues. For the most part, these proposals aim to remedy harms like the one that was experienced by Thomas Robins, who was not hired for a job because of incorrect information that an employer learned about him from the data search company Spokeo.[[150]](#footnote-150)

# Reforms for Information Services:

In addition to the proposals that respond specifically to the risks posed by the data broker industry, experts have proposed 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.[[151]](#footnote-151) Calo and others have proposed that companies offer a tracking-free version of their service that consumers can purchase.[[152]](#footnote-152) Many, including members of Congress, have called instead for the creation of universal “opt-out” provisions for consumers to refuse online tracking.[[153]](#footnote-153) Similarly, many scholars have proposed reforms to the increasingly dated statutory privacy protections described in Part I.[[154]](#footnote-154)

In addition to these commonly articulated proposals, scholars typically line up behind (or critique) an array “good data practices” frameworks, such as the Fair Information Practice Principles (FIPP) framework.[[155]](#footnote-155) The FTC articulated its Privacy By Design (PBD) principles in 2012, which calls on companies to delete no longer needed consumer data, as well as allow consumers to access their data and, when appropriate, allow consumers to change or delete information that companies posses.[[156]](#footnote-156) These principles are neither wholly novel[[157]](#footnote-157) nor without criticism, either that reflects existing ideological divides by critiquing the attempts by regulatory agencies to regulate internet companies,[[158]](#footnote-158) or because the frameworks themselves are outdated given the rapid expansion of data and how they are used.[[159]](#footnote-159)

These proposals are unlikely to remedy the problem of insider control, which emerges from the many actors that hold the amalgamation of a person’s online activity. None would prevent a wide array of actors from trading data about consumer habits, behaviors, and activities to other consumers.

We should remain skeptical that Congress will expand the scope FERPA, HIPAA, GLBA, and related statutes to prevent the trading of digital information about consumer purchases, intellectual capacities, and physiological information.[[160]](#footnote-160) Even less likely is the possibility of new legislation that would push U.S. commercial privacy law towards a European model (as many have recommended).[[161]](#footnote-161) Federal statutory privacy law remains has unchanged despite the rampant commodification of data, a near constant stream of embarrassing data breaches and leaks, and an increasingly lengthy list of documented privacy harms.[[162]](#footnote-162) With one narrow exception,[[163]](#footnote-163) Congress has not passed a statute related to privacy in more than a decade.[[164]](#footnote-164) It is also worth noting the federal statutory reforms have been notoriously poorly designed to combat future privacy threats. We should not expect new Congressional enactments to not struggle with the weaknesses of swift obsolescence, dilution by industry lobbying, or the well-documented tendency to target specific technologies.[[165]](#footnote-165)

Additionally, products that block targeted advertising or some forms of digital tracking[[166]](#footnote-166) are unlikely to inoculate a user from the threat of insider control. There are significant economic incentives for online actors to track consumer activity (these incentives fuel the internet’s free pricing structure).[[167]](#footnote-167) These incentives to gather information on consumers lead to new tracking technologies (such as pixel beacon tacking),[[168]](#footnote-168) 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.[[169]](#footnote-169) This lag time is an inevitable consequence of a free market economy, and prevents technical opt-outs from protecting consumers from the threat of insider control.

Regulatory FIPP or PBD frameworks are also incapable of preventing an insider control threat. These frameworks, along with coherent cyber security norms,[[170]](#footnote-170) 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 data weaponization: that our regime of data commodification allows vast quantities of consumer data to be placed in the hands of any interested individuals for a (cheap) price.

# Privacy-enhancing Consumer Technologies:

There are also an increasing number of technical methods for consumers to use the internet anonymously. A wide array of tools, from the Tor browser,[[171]](#footnote-171) to virtual private networks (VPN),[[172]](#footnote-172) to end-to-end encrypted messages,[[173]](#footnote-173) and encrypted desktops[[174]](#footnote-174) allow consumers to avoid tracking by most companies and, perhaps, some security agencies.

However, while these technologies may effectively mask a user’s identity when used to hide certain activities, they are less effective for a consumer’s online default use. Most websites run considerably slower on the Tor browser, and some features, including most video streaming options, cannot work without risking consumer privacy.[[175]](#footnote-175) Further, a larger obstacle is the simple fact that while certain, high information (and highly motivated) consumers could limit their vulnerability from insider control, most consumers will not take the steps necessary to shroud their activity[[176]](#footnote-176) (if they did, their actions would significantly disrupt the information economy).[[177]](#footnote-177)

# **Part V: “Information Fiduciaries” and “Sensitive Data”: Promises and Limits**

While most proposed reforms would offer minimal protection against insider attacks, two recent proposals, by Jack Balkin and Paul Ohm, if expanded, reveal possible new directions that could be more fruitful. Ohm and Balkin’s proposals each offer a path through longstanding legal challenges in privacy law. For Ohm, the obstacle is the “stuck” state of U.S. privacy law,[[178]](#footnote-178) through which an intervention that targets data understood to be particularly sensitive might realistically cut. For Balkin, the obstacle is meaningful privacy protection in the face of longstanding First Amendment obstacles, which an information fiduciaries approach could plausibly navigate.[[179]](#footnote-179) As presently constituted, neither offers any meaningful protection against insider control. However, Ohm’s proposal could be altered to account partially for the insider control problem, while Balkin’s proposal can, to some extent, be extended to respond to this new threat.

# Sensitive Data and Insider Control: The Beginnings of a Solution?

Ohm offers sensitive data as a solution to the otherwise inadequate protections of privacy law. Sensitive information is a “show stopper”[[180]](#footnote-180) that can summon robust protections out of otherwise lax privacy regulations, if data are sufficiently sensitive.[[181]](#footnote-181) For example, we see this feature of sensitive data in the FTC’s recommendation that data brokers establish opt-out provisions for most data, but opt-in protections for particular, sensitive data.[[182]](#footnote-182) A key feature of the “sensitive information” movement is that it frequently spurs statutory and regulatory action,[[183]](#footnote-183) while also being fueled significantly by private industry.[[184]](#footnote-184) Trade groups, like the Network Advertising Initiative and the Digital Advertising Alliance, and major companies (including Facebook and Google) offer their own, often divergent,[[185]](#footnote-185) guidelines on what information is sensitive and, unlike normal data, cannot be sold for profit.[[186]](#footnote-186)

Observing these features, Ohm argues that, for privacy advocates, sensitive data “may be the only game in town”[[187]](#footnote-187) that can secure protections where so many other proposals have failed. Ohm’s article surveys how laws come to recognize certain data as sensitive, and proposes that U.S. laws be revised to recognize as sensitive certain new forms of unprotected information.

Ohm’s sensitive data framework, if implemented, would not meaningfully protect consumers from the threat of insider control. Ohm proposes three new types of “sensitive” data—precise geolocation data; remote biometric data (including iris scan and facial recognition); and communications metadata.[[188]](#footnote-188) These types of data, particularly the latter, might provide an opening for insider attack. As Robinson Meyer observed in a 2014 *Atlantic* article, Facebook communications metadata can predict with surprising confidence when individuals will begin a relationship.[[189]](#footnote-189) Communications metadata can offer powerful maps of individual’s social networks and reveal changes in interactions, as well as points of closeness and tension. However, these unprotected data types are not the only, or necessarily the most important, data types that enable a threat of insider control. Data that provide deep insights into both behavior and interactions—for example, browser and purchase history, social network metadata, and—are particularly dangerous in the hands of peers. As presently constituted, data of these types would remain significantly unprotected under Ohm’s framework.

However Ohm offers two proposals that, if implemented, could yield value in the looming fight against the threat of insider control. First, Ohm argues that U.S. law should evolve to categorize certain types of data as sensitive data “no matter who holds it.”[[190]](#footnote-190) A core challenge for sensitive data as a partial remedy to insider 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.[[191]](#footnote-191) As discussed in Part I, the constant trading of data (to say nothing of hacked and subsequently leaked data) removes the teeth from most U.S. sensitive data laws. Ohm calls for a significant expansion of U.S. law (past the E.U. sensitive data laws), arguing that for certain types of sensitive information, “we should extend privacy protection regardless of the specific relationship.”[[192]](#footnote-192)

Second, 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.’”[[193]](#footnote-193) 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.[[194]](#footnote-194) While technical capacity has traditionally limited one’s capacity 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,[[195]](#footnote-195) enable companies to capture and separate sensitive data from vast, unstructured collections. Google researches, for example, have used machine-learning techniques to distinguish automatically flu symptoms from other search queries analyzed from the “billions of individual searches from 5 years of Google web search logs.”[[196]](#footnote-196) The power of these new tools underscores the need to consider possible affirmative protections requirements on unstructured data.

If implemented, these proposals might reduce certain insider control manifestations (such as efforts to manipulate individuals based on insights gleaned from social network data). However, to meaningfully protect consumers from insider control, Ohm’s framework for understanding what makes data sensitive would need to be reformulated to account for the capacity of peers to use data to manipulate the decisions of others. Additionally, the types of data that Ohm identifies as sensitive would need to be significantly expanded.

# Information Fiduciaries and Insider Control: A Second Path Forward?

Like Ohm, Balkin also looks to jumpstart privacy scholarship by arguing that there exists an implied fiduciary relationship[[197]](#footnote-197) between consumers and data holders that avoids both First Amendment[[198]](#footnote-198) and, in particular, freedom of contract[[199]](#footnote-199) barriers that doom many proposed privacy reforms.[[200]](#footnote-200)

Balkin argues that, much as doctors and lawyers owe a common law duty of loyalty and confidentiality to their clients and patients, so too should information services and service providers[[201]](#footnote-201) (information fiduciaries) owe certain duties of loyalty and care to their customers.[[202]](#footnote-202) Under Balkin’s proposal, certain duties of loyalty and care would 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.”[[203]](#footnote-203) Under the framework that Balkin maps, each of these entities that control consumer data would owe consumers to some degree fiduciary obligations.[[204]](#footnote-204)

As with Ohm’s sensitive data proposal, Balkin’s information fiduciaries framework is ill-suited in its current form to protect against the threat of insider control. Balkin’s framework is designed to protect consumers from direct ill-treatment from the companies that initially collect their data,[[205]](#footnote-205) rather than the indirect insider abuses that data transactions enable. Further, Balkin does not discuss the intersection of fiduciary obligations and data sale or third party data access in his article, or otherwise address the possibility that data could be harmful outside of the person to whom the user initially entrusts the data. The fiduciary obligations that Balkin discusses at length do not offer protection against the threat of insider control.

Nonetheless, Balkin’s framework can be extended to offer certain important footholds that could help to combat the threat of insider control. Balkin’s framework 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.[[206]](#footnote-206) As the report notes, companies “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.”[[207]](#footnote-207) Contractual provisions, if made far more prevalent, could provide consumers with meaningful protection against the threat of insider control. Unlike many other harms associated with data broker practices,[[208]](#footnote-208) the threat of insider control is enabled 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, fiduciary obligations could credibly be expanded to require companies to store data securely, and restrict what third parties and data brokers may control, sell, and use. A broader construction of fiduciary obligations 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 manifestations information fiduciaries make to consumers that they may be trusted with consumer data.[[209]](#footnote-209)

# **Part VI: Doctrinal Shifts in Light of Insider Control**

Protecting consumers from the threat of insider 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 insider 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 decisive answer to this threat that remains consistent with U.S. law. Given the global and diffused character of the internet, even outlawing the sale of data by U.S. firms to individuals would not produce a realistic solution. (And such an intervention would likely be unconstitutional.) As this paper is the first treatment on this type of privacy harm, it is inevitable that scholars will propose new and likely more effective of policy remedies in the years ahead. However, Part V offers a multi-layered set of ex ante and ex post doctrinal shifts that, if implemented, would likely offer meaningful protection for consumers against the threat of insider control.

# Congressional Privacy Reforms:

Congress could make an array of changes to existing Federal statutes and, as a result, meaningfully limit (but not eliminate) the threat of local control.[[210]](#footnote-210) However these changes are unlikely, due to the fact that data sale has become such an important part of the internet economy, and the difficulty inherent in mounting a major lobbying campaign. While updating existing privacy rules 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 related to one’s health or education. Accordingly, this Note favors these legislative proposals with a caution that the economic consequences have yet to be examined.

Congress nonetheless should pass legislation that unambiguously protects consumers from a significant insider control threat: e-communications. The SCA prohibits ISPs from selling the contents of some communications to third parties, and the FCC’s new rules extend these protections to all messages collected by ISPs, these laws do not limit sales by non-ISP information services like most commercial websites and applications.[[211]](#footnote-211) Congress should close this gap by passing strong legislation that prohibits companies from selling to third parties the content or metadata of emails, messages, and other forms of online communications. Already, we have seen political interest in some elements of these reforms. The House of Representatives recently passed the Email Privacy Act, 419-0,[[212]](#footnote-212) although the bill is hardly perfect—it does not address the use or sale of communications content or metadata by private companies, and is not broadly designed to account for the many new forms of online communications. An amended and extended Communications Privacy Act would close this gap and provide meaningful protection against the abuse of a particularly dangerous type of data. Such a law would reflect both Congress’s longstanding preference for narrow privacy reforms and also reflect longstanding U.S. commitment to the privacy of written expression.[[213]](#footnote-213)

# Privacy Intrusion Reconsidered:

This Note recommends that the intrusion tort be understood in light of contemporary technological sensibilities. The Second Restatement of Torts defines intrusion: “[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.”[[214]](#footnote-214) Courts to date have held that privacy incursions that result from data sale fall well short of the “highly offensive” standard. However, insider control poses new questions that will almost certainly divide common law courts in the years ahead. First, courts will need to weigh whether a user can claim that she still has a privacy interest in the records of data that are legally controlled by a host of third parties. This Note recommends that courts begin to view this threshold question more favorably.

There are number of factors that weigh in favor of recognizing a privacy interest in data even as it is controlled by third parties. First, it is a structural feature of the digital age that one’s personal data, over which it was once possible to exercise sole control, is now inevitably controlled third parties.[[215]](#footnote-215) Whatever one does online, there are usually many entities—among them the commercial ISP, third party advertisers, and host websites (as well as an array of state intelligence agencies)—that control the records of that activity. This Note argues that users should not lose a right to consider one’s most intimate data private simply because the structure of the internet does not allow a person to operate online without some actors gaining control over the data.[[216]](#footnote-216) This view reflects doctrinal rumblings in the Supreme Court, which, while not binding, have begun to push back on the idea a third party’s possession of a user’s data does not necessarily mean that others’ (the state or individuals) access to that data does not violate the user’s privacy.[[217]](#footnote-217) This perspective is also supported by increasingly clear evidence of public opinion.[[218]](#footnote-218)

However, important counterarguments can be raised in response to this recommendation. This Note recommends, in effect, that courts should recognize a person’s privacy interest in information that is legally controlled by another entity.[[219]](#footnote-219) This recommendation may constitute a significant, and perhaps unrealistic, stretching of property law. Additionally, if courts began to reach those conclusions, there could be significant economic consequences if the value of data plummeted in response to different courts identifying privacy interests in otherwise controlled data.

This Note is skeptical that certain common cases recognizing a valid privacy interest would have more than a marginal impact on the market for digital information. A move by common law courts to recognize a privacy interest in data stored, for example, on the cloud would still require privacy victims to realize they had suffered a privacy intrusion (and want to sue). This bar, along with the limited economic consequences for the commercial data controller in a tort claim against an individual intruder, suggests that common law courts could begin to recognize an intrusion claim against individuals that covertly purchase certain, sensitive information, without disrupting the broader market for data. At the same time, a doctrinal shift along these lines could provide a possible deterrent on individuals who look to purchase data on their peers.[[220]](#footnote-220)

In order to recognize an intrusion tort for certain instances of insider controllers, courts would also need to find that the intruder’s lawful purchase and access of data was highly offensive. This question allows for legitimate disagreement, and courts should continue to debate and disagree on a case-by-case basis.[[221]](#footnote-221) At the same time, however, certain courts have held the “highly offensive” standard to an unreasonably high bar—for example, some courts have read “highly offensive” not to apply to an individual’s unauthorized access of another’s email.[[222]](#footnote-222) This Note argues that such an interpretation of highly offensive is unreasonable in the current digital environment.

# Balkin and Ohm Frameworks as ex post Protections:

Balkin and Ohm offer a pair of theoretical avenues to protect consumers from the threat of insider control after data has been collected. Both scholars propose frameworks that can be extended or altered to protect consumers from this new context 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 altered to construe a far wider category of information as sensitive. U.S. laws that govern 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. By changing how we conceive or should conceive of sensitive information to include data of these types, a far broader array of information could trigger regulatory protections after it has been collection. For example, sensitive data should trigger certain rules for companies handling these data after it has been collected—including the FIPPs of “purpose specification” and “use limitation,” which can necessarily 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 valid purpose.[[223]](#footnote-223)

There remain clear economic risks in the revised Ohm framework that this Note proposes. By radically expanding the types of data that regulators should consider sensitive, U.S. companies might quickly find themselves in control of data that immediately triggers economically burdensome safeguards that threaten a companies’ viability. Over-protective regulations could also curb the development of many important, pro-societal benefits that stem from the efficient commercial access to consumer data.[[224]](#footnote-224)

Balkin’s framework should be extended, consistent to its theoretical underpinnings, to require companies to have duties to protect consumer data from the threat of insider control. Without distorting the tenets of Balkin’s framework, fiduciaries should be required to limit the risk of insider control by selling data only in the context of tightly constrained contractual rules against re-identification and subsequent, purpose-flexible resale. Such duties would limit the unconstrained access that brokers would have to consumer data, limiting their ability to sell data to individuals seeking the data of particular persons.[[225]](#footnote-225)

# Privacy Opt-ins for Data Sale:

Contract law remains one of the most fertile ground for privacy reform, including in the context of data brokers. The FTC’s Section 5 enforcement actions take aim at companies that lack privacy policies and at those whose actual policies deviate from their stated policies.[[226]](#footnote-226) 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.[[227]](#footnote-227) However, opt-outs also come with risks, including a consumer’s implied, unwitting, consent to policies that may prove detrimental.[[228]](#footnote-228) In order to avoid setting consumers up for bad “deals,” the FTC should explore mandating a narrow set of clear, logistically straight-forward opt-in provisions regarding the sale of collected data. These provisions could extend the FCC ISP requirements to web browsers generally—a step recommended by a Republican FCC Commissioner in light of the FCC’s recent ruling.[[229]](#footnote-229) Requiring that companies receive from consumers clear, meaningful consent, not tied to a reduction or denial of service, will provide a strong mechanism for consumers to protect against the threat of insider control.

These proposed changes to privacy doctrine will not inoculate consumers from the threat of insider control nor are they immune to criticism. However, the combination of each can significantly reduce the threat that consumers currently experience from insider control and offer a way for privacy law to protect consumers while avoiding significant disruption to the economic landscape around data.

# **Conclusion:**

This paper attempts to offer a new rationale for why digital privacy is crucial in the 21st century: that under the current regime, your most intimate information can inevitably be acquired by someone in your social or professional circles who wants to exercise control over your most personal data. The internet age has been founded on a Wild West of privacy abuse—as the intimate information of a generation of internet users has been taken, largely without their knowledge or ability to refuse. Scholarship to date has failed to consider the implications of this threat, and no policy can serve as a silver bullet against the problem of insider control. However, insider control reveals necessary reforms to doctrine, which, if implemented, will significantly reduce this threat.

Taking a step back, the threat of insider control appears to offer new evidence of digital privacy’s oft-overlooked *contextual* features. As society has moved from the analog to digital age—with clocks replaced by the cell phone and the letter replaced by the email—individuals have lost the ability to exercise sole control over who access to their vast majority of their private information. It is a structural feature of our digital age that the records of digital activity are controlled by an array of actors, form private ISPs to state intelligence services, which exist beyond the consumer’s ability to meaningfully influence. Many scholars and consumers have questioned whether privacy can exist in such an environment.

I would argue that the threat of insider control demonstrates that privacy *can* exist. Insider control shows that privacy violations are inherently context dependent: data that might be harmless in the hands of an entity like Facebook, Google, or the NSA, can be dangerous if possessed by a professional or social rival (or a con artist). Ultimately, any legal intervention that hopes to protect consumers from the threat of insider control must recognize this contextual feature of digital privacy—that what is important is not only *what* others may know but also *who* may know it.

1. *See, e.g.*,Federal Trade Comm’n, FTC Data Brokers: A Call for Transparency and Accountability (May, 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter FTC Data Brokers]. [↑](#footnote-ref-1)
2. *See* FTC Data Brokers 3. [↑](#footnote-ref-2)
3. FTC Data Brokers 8. [↑](#footnote-ref-3)
4. FTC Data Brokers 9. [↑](#footnote-ref-4)
5. 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/. [↑](#footnote-ref-5)
6. 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; *see also* FTC Data Brokers 17 (describing self-imposed contractual protections that some brokers unilaterally adopt). [↑](#footnote-ref-6)
7. *See, e.g.*,Emily Steel, *Financial worth of data comes in at under a penny a piece*, Financial Times (June 12, 2013 8:11 PM), http://www.ft.com/intl/cms/s/0/3cb056c6-d343-11e2-b3ff-00144feab7de.html. [↑](#footnote-ref-7)
8. FTC Data Brokers 14. [↑](#footnote-ref-8)
9. FTC Data Brokers 14. [↑](#footnote-ref-9)
10. *See, e.g.*, David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 Ohio N.U. L. Rev. 493, 498 (2016) ; 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; Ashley Keumpel, Comment, The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry, 36 Nw. J. Int’l L. & Bus. 207 (2016). [↑](#footnote-ref-10)
11. *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.*,Richard A. Posner*, The Economics of Privacy*, 71 Am. Econ. Rev. 405 (1981); Robert H. Bork, *The Right to Privacy: The Construction of a Constitutional Time Bomb*, *in* Principles of Constitutional Interpretation 311 (1990). [↑](#footnote-ref-11)
12. *See, e.g.*, Spokeo v. Robbins, 136 S.Ct. 1540 (2016) (vacating and remanding 9th Circuit ruling as failing to satisfy standing requirements); *see also* *In Re Google, Inc. Privacy Policy Litigation*, 2013 WL 6248499, \*3 (N.D. Cal. 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*, at 1132 (“A privacy harm must be ‘cognizable’, ‘actual,’ ‘specific,’ ‘material,’ ‘fundamental,’ or ‘special’ a court will consider awarding compensation.”). [↑](#footnote-ref-12)
13. *See, e.g.*, Stewart A. Baker, Skating on Stilts: Why We Aren’t Stopping Tomorrow’s Terrorism (2012); Amatai 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 . . . .”). [↑](#footnote-ref-13)
14. *See, e.g.*,Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 493 (2006) (providing a “comprehensive and concrete” description of harms associated with information collection, processing, dissemination, and intrusion). [↑](#footnote-ref-14)
15. *Id.*  [↑](#footnote-ref-15)
16. *See, e.g.*, Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating “Haves” from “Have-Nots”*, 2014 Mich. St. L. Rev. 1411; *see also* Ashley Keumpel, Comment, The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry, 36 Nw. J. Int’l L. & Bus. 207 (2016) (underscoring the discriminatory implications of data commoditization). [↑](#footnote-ref-16)
17. Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 Antitrust L.J. 121, 153-155 (2015). Nevertheless, many 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). [↑](#footnote-ref-17)
18. *See, e.g.*, Solove, *supra*,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.”); Paul M. Shwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 1656 (1999); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1426 (2000). [↑](#footnote-ref-18)
19. *See, e.g.*, 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); Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights (May 2016), https://www.whitehouse.gov/sites/default/files/microsites /ostp/2016\_0504\_data\_discrimination.pdf; 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 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2778165##.

    [↑](#footnote-ref-19)
20. *See, e.g.*,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/; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016); 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; Bruce Schneier, *Why Uber’s ‘god view’ is creepy*, CNN (Dec. 4, 2014 8:03 AM EST), http://www.cnn.com/2014/12/04/opinion/schneier-uber-privacy-issue/index.html. [↑](#footnote-ref-20)
21. 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* at 1187-94 (describing Uber’s efforts to “dig up dirt” on a critical Buzzfeed reporter); Laurie Seagall, *Ashley Madison users now facing extortion*, CNNMoney (Aug. 21, 2015), http://money.cnn.com/2015/08/21/technology/ashley-madison-users-extorted/. [↑](#footnote-ref-21)
22. *See, e.g.*,Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 493 (2006) (providing a “comprehensive and concrete” description of harms associated with information collection, processing, dissemination, and intrusion); Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. Econ. & Pol’y 1 (2015) (arguing that the various data practices will increase the likelihood of identity fraud; modeling by companies that is discriminatory or otherwise harmful to consumers; consumer manipulation; and the “forced” revelation of consumer data). *See also* 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. [↑](#footnote-ref-22)
23. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L. J. 1131 (2011) (describing the boundaries of “objective”—involving financial, dignitary, or other tangible loss—and “subjective”—involving psychological ill-ease or distress—harms). [↑](#footnote-ref-23)
24. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 493 (2006) (“[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, THE HOLLYWOOD REPORTER (Dec. 17, 2014), http://www.hollywoodreporter.com/news/sony-hack-fallout-executives-afraid-758506.

    [↑](#footnote-ref-24)
25. *See, e.g.*, Shwartz, *supra*, 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.”); Cohen, *supra*, at 1426 (“[P]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream.”). [↑](#footnote-ref-25)
26. *See, e.g.*,Thomas M. Leard & Paul H. Rubin, *Big Data, Privacy, and the Familiar Solutions*, 11 J.L. Econ. & Pol’y 1, 20-22 (2015) (describing how firms use big data to manipulate consumers); 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). [↑](#footnote-ref-26)
27. *See, e.g.*, Bruce Schneier, *Candidates won’t hesitate to use manipulative advertising to score votes*, Guardian (Feb. 4, 2016 6:45 AM EST), https://www.theguardian.com/commentisfree/2016/feb/04/presidential-election-voter-data-manipulative-advertising-privacy. [↑](#footnote-ref-27)
28. *See, e.g.*, Balkin, 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); Laurie Seagall, *Ashley Madison users now facing extortion*, CNNMoney (Aug. 21, 2015), http://money.cnn.com/2015/08/21/technology/ashley-madison-users-extorted. [↑](#footnote-ref-28)
29. *See, e.g.*, *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (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). [↑](#footnote-ref-29)
30. *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, 2091-2093 (2015) (describing the privacy interest in avoiding social sorting and discrimination); Leard & Rubin, *supra*, at 18-20 (describing how bid data can be used to discriminate); Margaret Hu, *Big Data Blacklisting*, 67 Fla. L. Rev. 1735 (2015). [↑](#footnote-ref-30)
31. Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 Wake Forest L. Rev. 433, 454-459 (2014) (describing how the prominence of data sale and bulk data brokers exacerbates data vulnerability); Leard & Rubin, *supra*, at 12-17 (describing the increase in data breaches and cyber attacks that has accompanied the increase of online commercial activity). [↑](#footnote-ref-31)
32. Daniel J. Solove, *Identity Theft****,*** *Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1229 (2003). [↑](#footnote-ref-32)
33. *See, e.g.,* Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 Santa Clara High Tech. L.J. 483 (2015); Michelle M. Christovich, Note, Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information, 38 Hastings Comm. & Ent L.J. 91 (2016). [↑](#footnote-ref-33)
34. *See supra* note 10. [↑](#footnote-ref-34)
35. Vladeck, *supra*, at 501-12. [↑](#footnote-ref-35)
36. *Cf* Slade Bond, *Doctor Zuckerberg: Or, How I Learned To Stop Worrying And Love Behavioral Advertising*, 20-Fall Kan. J.L. & Pub. Pol’y 129 (2010). [↑](#footnote-ref-36)
37. Lipman, *supra*, at 781-2 (2016). [↑](#footnote-ref-37)
38. Schmitz, *supra*. [↑](#footnote-ref-38)
39. *See, e.g.*,Daniel J. Solove, Information Privacy Law 790-798 (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). [↑](#footnote-ref-39)
40. *See* Fair Credit Reporting Act, Pub. L. No. 91-508, §106, 84 Stat. 1114, 1128 (1970) (codified as amended in scattered sections of 15 U.S.C.). [↑](#footnote-ref-40)
41. *See, e.g.*, Equifax, *FCRA Summary of Rights*, https://www.equifax.com/privacy/fcra. [↑](#footnote-ref-41)
42. *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012). [↑](#footnote-ref-42)
43. *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, and 42 U.S.C.). [↑](#footnote-ref-43)
44. *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. [↑](#footnote-ref-44)
45. *See* 18 U.S.C., ch. 121, §§2701-2712. [↑](#footnote-ref-45)
46. *See* *id.* [↑](#footnote-ref-46)
47. *See, e.g.*, Tene, *supra*, at 1217(“At best, the current framework strains to keep up with new developments; at worst, it has become irrelevant.”). [↑](#footnote-ref-47)
48. *See, e.g.*, Ohm, *supra*, 1191. [↑](#footnote-ref-48)
49. Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 Penn St. L. Rev. 777, 788 (2016).

    [↑](#footnote-ref-49)
50. *Id.* [↑](#footnote-ref-50)
51. Ohm, *supra*, at 1190 n. 362. [↑](#footnote-ref-51)
52. *Id.* at 1140. [↑](#footnote-ref-52)
53. *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 (2nd Cir. 2016) (Lynch, J. concurring) (pointing to Kerr’s critiques from more than 12 years prior as evidence of pressing need for Congress to revisit the statute). [↑](#footnote-ref-53)
54. *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, and 42 U.S.C.). [↑](#footnote-ref-54)
55. *See, e.g.*, *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (2010). [↑](#footnote-ref-55)
56. *See, e.g.*, Kerr, *supra*. [↑](#footnote-ref-56)
57. Ohm, *supra*, at 1192 (quoting COPPA). [↑](#footnote-ref-57)
58. 16 C.F.R. pt. 312. [↑](#footnote-ref-58)
59. California Social Media Privacy Act of 2012, Cal. Lab. Code §980 (West 2012). [↑](#footnote-ref-59)
60. *See* Cal. Civ. Code § 1798.83(a) (2006); Cal. Civ. Code § 1798.83(e)(6)(A) (2006); [↑](#footnote-ref-60)
61. Cal. Civ. Code § 1798.83(e)(2); *see* Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 Penn St. L. Rev. 777, 794 (2016). [↑](#footnote-ref-61)
62. *See, e.g.*,Paul Ohm, *supra*, at 1127 n.3 (2015); 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). [↑](#footnote-ref-62)
63. *See, e.g.*, William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 383-343 (1960). [↑](#footnote-ref-63)
64. Restatement (Second) of Torts § 652 (Am. Law Inst. 1977) (emphasis added). [↑](#footnote-ref-64)
65. *See supra* note 12. [↑](#footnote-ref-65)
66. 341 N.E.2d 337 (Ohio Ct. App. 1975). [↑](#footnote-ref-66)
67. *Id.* at 339. [↑](#footnote-ref-67)
68. Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. 1995). [↑](#footnote-ref-68)
69. 816 A.2d 1001 (2003). [↑](#footnote-ref-69)
70. The resident sought at different times the date of birth, social security number, home address, for one person, and paid over $200 for these pieces of information. *See id.* at 1006-07. [↑](#footnote-ref-70)
71. *Id.* at 1006-07. [↑](#footnote-ref-71)
72. Brian Fung & Craig Timberg, *The FCC just passed sweeping new rules to protect your online privacy*, Wash. Post (Oct. 27, 2016), https://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.”). [↑](#footnote-ref-72)
73. Press Release, Tom Wheeler, FCC Chairman, *Protecting Privacy for Broadband Consumers* (Oct. 6, 2016), https://www.fcc.gov/news-events/blog/2016/10/06/protecting-privacy-broadband-consumers. [↑](#footnote-ref-73)
74. Fung & Timberg, *supra*. [↑](#footnote-ref-74)
75. Mike Masnick, *As Expected, FCC Passes Modest Privacy Rules for Broadband Providers, ISPs Act Like World Has Ended*, techdirt (Oct. 27, 2016). https://www.techdirt.com/articles/20161027/11361035900/as-expected-fcc-passes-modest-privacy-rules-broadband-providers-isps-act-like-world-has-ended.shtml. [↑](#footnote-ref-75)
76. *Cf.* Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24, 5608-09, para. 25 (“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.”). [↑](#footnote-ref-76)
77. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 600, 610 (2014). [↑](#footnote-ref-77)
78. 15 U.S.C. §§ 45, 52 (2012); *see* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practice*s, 48 San Diego L. Rev. 809, 811 (2011) (tracing the FTC’s evolving role in the enforcement of consumer protection). [↑](#footnote-ref-78)
79. Electronic Privacy Information Center, *In re*: *Snapchat*, https://epic.org/privacy/internet/ftc/snapchat/#response. [↑](#footnote-ref-79)
80. 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/. [↑](#footnote-ref-80)
81. Press Release, Federal Trade Commission, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (Nov. 29, 2011). https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep. [↑](#footnote-ref-81)
82. *See* FTC Data Brokers 16-17. [↑](#footnote-ref-82)
83. *United States v. Choicepoint Inc.*, (N.D. Ga), Jan. 26, 2006. 2003-2008 CCH Dec. ¶ 100-290. [↑](#footnote-ref-83)
84. CQ Roll Call Staff, *FTC cites 2015 successes in privacy, data security actions*, 2016 WL 2759289 (Apr. 6, 2016). [↑](#footnote-ref-84)
85. *Cf.* Lipman, *supra*, 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 are very limited.”). [↑](#footnote-ref-85)
86. *Id.* at 789. [↑](#footnote-ref-86)
87. 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. [↑](#footnote-ref-87)
88. 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/ (“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.”) [↑](#footnote-ref-88)
89. Vladeck, *supra*, 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.”). [↑](#footnote-ref-89)
90. *See* FTC Data Brokers 11-13. [↑](#footnote-ref-90)
91. *See id.* at 13. [↑](#footnote-ref-91)
92. *See id.* at 13-14. [↑](#footnote-ref-92)
93. *See id.* at 14. [↑](#footnote-ref-93)
94. *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 (“As shady as it might sound, the entire industry is completely legal.”). [↑](#footnote-ref-94)
95. *See, e.g.*,Neal Ungerleider, *Yes, Political Campaigns Follow Your Browser History*, FastCompany (Nov. 5, 2013 9:30 AM), https://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 . . . “). [↑](#footnote-ref-95)
96. *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.” [↑](#footnote-ref-96)
97. *See e.g.*, Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, Propublica (June 11, 2011 11:45 AM), https://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. [↑](#footnote-ref-97)
98. *See* FTC Data Brokers 23. J.L. Econ. & Pol'y [↑](#footnote-ref-98)
99. *Id.* at 34. [↑](#footnote-ref-99)
100. *Id.* (emphasis added). [↑](#footnote-ref-100)
101. *See* FTC Data Brokers 17. [↑](#footnote-ref-101)
102. *See id.* at 17. For more on how these contractual provisions could be useful hooks to prevent insider control, see *infra* Part IV. [↑](#footnote-ref-102)
103. Emily Steel, *Disparate network of companies is difficult to bring to heel*, Financial Times (June 12, 2013 8:11 PM), http://www.ft.com/intl/cms/s/0/a0cb7b5e-d343-11e2-b3ff-00144feab7de.html. [↑](#footnote-ref-103)
104. *See, e.g.*, Arun Sundararaian et al.,Research Commentary, *Information in Digital, Economic, and Social Networks*, 24 Information Systems Research 883 (2013) (providing a synopsis of recent scholarship across social science disciplines on the effects of digital information on digital, economic, and social networks); Sinan Aral et al., Productivity Effects of Information Diffusion in Networks, MIT Sloan School Working Paper 4683-08, 1 (2007), http://dspace.mit.edu/bitstream/handle/1721.1/65404/SSRN-id1085354.pdf;sequence=1 (finding distinct diffusion habits in the travel of information across companies and finding that “access to information strongly predicts the number of projects completed by each individual and the amount of revenue that person generates.”); James H. Fowlera & Nicholas A. Christakis, *Cooperative Behavior Cascades in Human Social Networks*, 107 PNAS 5334 (2010) (demonstrating the lasting impact of behavioral and personality similarities on cooperative social interactions). [↑](#footnote-ref-104)
105. *See* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. Colo. L. Rev. 1117, 1154 (2013) [↑](#footnote-ref-105)
106. While Wu underscores the not-clarified legal state of insider attacks, and their difficulty to counter, neither Wu nor any other scholar has discussed this threat, its implications, and possible solutions. *See id*. [↑](#footnote-ref-106)
107. *Id.*  [↑](#footnote-ref-107)
108. *Id.* [↑](#footnote-ref-108)
109. *See, e.g.*, Cyril Tompkins, *Interdependencies, Trust and Information in Relationships, Alliances and Networks*, 26 Accounting, Organizations and Society 161 (2001) (describing the relationship between information access, asymmetries, and the development of trust in social networks). [↑](#footnote-ref-109)
110. *Cf.* Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness (2009) (arguing on a macro level how experts can offer certain choice architectures that drastically effects consumer decision making). [↑](#footnote-ref-110)
111. *See Id.*; Digital Advertising Alliance, Application of self-Regulatory Principles to the Mobile Environment (2013), http://www.aboutads.info/DAA\_Mobile\_Guidance.pdf; Digital Advertising Alliance, Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (2015), http://www.aboutads.info/sites/default/files/DAA\_Cross-Device\_Guidance-Final.pdf. [↑](#footnote-ref-111)
112. FTC Data Brokers 14. [↑](#footnote-ref-112)
113. *Id.* [↑](#footnote-ref-113)
114. *See, e.g.*, Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. Mo. B. 76 (2016). [↑](#footnote-ref-114)
115. *Cf.* Zero Days (2016) (“If you can spy on a network, you can manipulate it”). [↑](#footnote-ref-115)
116. *See, e.g.*,Emily Steel, *Companies scramble for consumer data*, Financial Times (June 12, 2013 8:11 PM), 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*, Financial Times (June 12, 2013 8:11 PM), http://www.ft.com/intl/cms/s/0/a0cb7b5e-d343-11e2-b3ff-00144feab7de.html. [↑](#footnote-ref-116)
117. Emily Steel, *Financial worth of data comes in at under a penny a piece*, Financial Times (June 12, 2013 8:11 PM), http://www.ft.com/intl/cms/s/0/3cb056c6-d343-11e2-b3ff-00144feab7de.html. [↑](#footnote-ref-117)
118. *Id.* [↑](#footnote-ref-118)
119. *Id.* [↑](#footnote-ref-119)
120. *Id.* [↑](#footnote-ref-120)
121. *See* Emily Steel et al., *How much is your personal data worth?*, Financial Times (June 12, 2013 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html. [↑](#footnote-ref-121)
122. *See, e.g.*,Neal Ungerleider,*Yes, Political Campaigns Follow Your Browser History*, FastCompany (Nov. 5, 2013 9:30 AM), https://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) . . . .). [↑](#footnote-ref-122)
123. *See, e.g.*, *Fact Sheet 41: Data Brokers and Your Privacy*, Privacy Rights Clearinghouse (May 2016), https://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). [↑](#footnote-ref-123)
124. *See* Eugene Volokh, *Freedom of Speech and 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). [↑](#footnote-ref-124)
125. *See, e.g.*, FTC Data Brokers 14. [↑](#footnote-ref-125)
126. *See* HIPAA Privacy Regulations, 45 CFR § 64.514 (b), (c). [↑](#footnote-ref-126)
127. Health and Human Services, *The De-Identification Standard*, http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#standard. [↑](#footnote-ref-127)
128. *See, e.g.*, Jonathan Camhi, *Barclays Plans to Sell Anonymized Datat 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?. [↑](#footnote-ref-128)
129. *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/. [↑](#footnote-ref-129)
130. *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. [↑](#footnote-ref-130)
131. *See, e.g.*, Bryan Clark, *Comcast: ISPs should be able to sell your Web history to advertisers*, TNW (Aug., 2016), http://thenextweb.com/insider/2016/08/03/comcast-isps-should-be-able-to-sell-your-web-history-to-advertisers/; Michael H., *AT&T planning to sell your anonymous usage data to advertisers*, PhoneArena (July 3, 2013), http://www.phonearena.com/news/AT-T-planning-to-sell-your-anonymous-usage-data-to-advertisers\_id44890. [↑](#footnote-ref-131)
132. Swati Khandelwal, *ISPs Sell Your Data To Advertisers, but FCC Has a Plan to Protect Privacy*, The HAcker News (Mar. 11, 2016), https://thehackernews.com/2016/03/isp-sells-data-to-advertisers.html. This activity is now subject to the recent FCC rules requiring ISPs to gain consumer consent before they sell data. [↑](#footnote-ref-132)
133. *See e.g.*, Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, Propublica (June 11, 2011 11:45 AM). [↑](#footnote-ref-133)
134. *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.”) [↑](#footnote-ref-134)
135. *See, e.g.*, Scott Berinato, *There’s No Such Thing As Anonymous Data*, HArvard Business Review (Feb. 09, 2015), https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data. [↑](#footnote-ref-135)
136. *See* Bin Zhou et al., *A Brief Survey on Anonymization Techniques for Privacy Preserving Publishing of Social Network Data*, 10 ACM SIGKDD Explorations Newsletter 12 (2008), https://www.cs.sfu.ca/~jpei/publications/SocialNetworkAnonymization\_survey.pdf. [↑](#footnote-ref-136)
137. Xuan Ding et al., *A Brief Survey on De-anonymization Attacks in Online Social Networks*, 2010 International Conference on Computational Aspects of Social Networks, at 614. [↑](#footnote-ref-137)
138. Arvind Narayanan and Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, in *EEE Symposium on Security and Privacy (S&P)* (2008), https://www.cs.utexas.edu/~shmat/ shmat\_oak08netflix.pdf. [↑](#footnote-ref-138)
139. *Id.* at 12. [↑](#footnote-ref-139)
140. Sarah Jamie Lewis, Please Stop Releasing "Anonymized" Datasets, Linkedin Pulse (Jan. 25, 2016), https://www.linkedin.com/pulse/please-stop-releasing-anonymized-datasets-sarah-jamie-lewis. [↑](#footnote-ref-140)
141. *See* Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014); Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating “Haves” from “Have-Nots*,*”* 2014 Mich. St. L. Rev. 1411 (2014). [↑](#footnote-ref-141)
142. *Schmitz*, *supra,* at 1458. [↑](#footnote-ref-142)
143. FTC Data Brokers 51-2. [↑](#footnote-ref-143)
144. FTC Data Brokers 52. For more on sensitive data frameworks as a possible response to the threat of insider control, see *infra* Part IV. [↑](#footnote-ref-144)
145. *See, e.g.*,Ashley Keumpel, Comment, The Invisible Middlemen: A Crtique and Call for Reform of the Data Broker Industry, 36 Nw. J. Int’l L. & Bus. 207 (2016); 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). [↑](#footnote-ref-145)
146. *See* Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 Penn St. L. Rev. 777, 796-86 (2016). [↑](#footnote-ref-146)
147. *See, e.g.*, Jugpreet Mann, Note, Small Steps for Congress, Huge Steps for Online Privacy, 37 Hastings Comm. & Ent. L.J. 365, 387 (2015). [↑](#footnote-ref-147)
148. Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 Ind. L.J. 267, 347 (2016). [↑](#footnote-ref-148)
149. *See id.* at 346-49. [↑](#footnote-ref-149)
150. *See, e.g.*, Electronic Privacy Information Center, *Spokeo, Inc. v. Robins*, https://epic.org/amicus/spokeo/. [↑](#footnote-ref-150)
151. 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%C80%99s-chair/130819bigdataaspen.pdf (“The emergence of big data are similarly breathtaking and potentially game changing. But the challenges it poses to consumer privacy are familiar . . . . The solutions are also familiar.”). [↑](#footnote-ref-151)
152. *See, e.g.*,Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 95 (2014); Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. Econ. & Pol’y (2015). [↑](#footnote-ref-152)
153. *See e.g.*, Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information,* 74 Wash. L. Rev. 1033 (1999); Do Not Track Me Online Act, H.R. 654 (112); Do-Not-Track Online Act of 2011, S.913 (112); Do Not Track Kids Act of 2011, H.R. 1895 (112). [↑](#footnote-ref-153)
154. *See, e.g.*, Ohm, *supra*, at 1191; Jugpreet Mann, Note, Small Steps for Congress, *Huge Steps for Online Privacy*, 37 Hastings Comm. & Ent L.J. 365 (2015); Eugene E. Hutchinson, Note, Keeping Your Personal Information Personal: Trouble for the Modern Consumer, 43 Hofstra L. Rev. 1151 (2015); *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). [↑](#footnote-ref-154)
155. Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*,30 Berkeley Tech. L.J. 2073, 2101-06 (2015) (describing various Fair Information Principles and how they came to be articulated). [↑](#footnote-ref-155)
156. *Id.* at 23-24 (2012). [↑](#footnote-ref-156)
157. *See* Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. Econ. & Pol’y 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”); *see also* Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*,30 Berkeley Tech. L.J. 2073, 2101-06 (2015) (describing the scope of the OECD guidelines). [↑](#footnote-ref-157)
158. *See, e.g.*, Paul H. Rubin, *Regulation of Information and Advertising*, 4 Competition Policy Int'l, 169, 169-92 (2008) (arguing that the FTC has at times overprotected consumers with excessive regulation). [↑](#footnote-ref-158)
159. *See, e.g.*, 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); Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. Econ. & Pol’y 1, 26 (arguing that the commissioner’s recommendation are “ill suited to the world of big data”). [↑](#footnote-ref-159)
160. Further, even if Congress reformed existing statutes, other records of digital activity, such as what consumers read and watch, would not be affected. [↑](#footnote-ref-160)
161. *See, e.g.*, *See, e.g.*,Ashley Keumpel, Comment, The Invisible Middlemen: A Crtique and Call for Reform of the Data Broker Industry, 36 Nw. J. Int’l L. & Bus. 207 (2016); 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). [↑](#footnote-ref-161)
162. *See infra* Part II. [↑](#footnote-ref-162)
163. *See* the Genetic Information Nondiscrimination Act of 2008, H.R. 493, 110th Cong. §2 (2008). [↑](#footnote-ref-163)
164. *See* Ohm, *supra*, at 1125. [↑](#footnote-ref-164)
165. *See* Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 Yale J.L. & Tech. 24 (documenting examples of statutes that prove ineffective or stifling because they target particular technologies for reform). [↑](#footnote-ref-165)
166. *See, e.g.*,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), https://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), https://motherboard.vice.com/blog/now-you-can-see-what-websites-are-tracking-you-in-real-time. [↑](#footnote-ref-166)
167. *See, e.g.*, Lipman, *supra*, 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 references omitted);

     Emily Steel, *Companies scramble for consumer data*, Financial Times (June 12, 2013 8:11 PM); *How Many of Your Users Set “Do Not Track”?*, Quantable (Feb. 2, 2015), https://www.quantable.com/analytics/how-many-do-not-track/ (measuring the percent of users who opt-out of tracking as between 8 and 15%). [↑](#footnote-ref-167)
168. Joanna Geary, *Tracking the trackers: What are cookies? An introduction to web tracking*, Guardian (Apr. 23, 2012) (describing flash cookies and web beacons). [↑](#footnote-ref-168)
169. *See, e.g.*, Brian Barret, *Update Your Pokémon Go App Now to Fix That Privacy Mess*, Wired (July 12, 2016), https://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.”) [↑](#footnote-ref-169)
170. *See* Nat’l Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cyberframework. [↑](#footnote-ref-170)
171. *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. [↑](#footnote-ref-171)
172. *See, e.g.*, The\_Blode, Best Free Anonymous Surfice Services, gizmo’s freeware (May 2, 2015), http://www.techsupportalert.com/best-free-anonymous-surfing-service.htm. [↑](#footnote-ref-172)
173. *See, e.g.*,Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, Wash. Post (Sept. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering- default-encryption-blocking-police. [↑](#footnote-ref-173)
174. *See, e.g.*, *Tails: the amnesic incognito live system*, https://tails.boum.org/. [↑](#footnote-ref-174)
175. *See NoScript*, accessed from the Tor Browser. [↑](#footnote-ref-175)
176. *See* Kesan et al., *supra*. [↑](#footnote-ref-176)
177. *See,e.g.*, John E. Dunn, *Best 7 online privacy tools 2016 – VPNs, anonymous search, and browser secrecy*, TechWorld, 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.”) [↑](#footnote-ref-177)
178. *See* Ohm, *supra* at 1127. [↑](#footnote-ref-178)
179. *See, e.g.*,Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 STAN. L. REV. 1049, 1089 (2000) (arguing that the claim for governments to regulate speech of private concern to protect information privacy “is theoretically unsound . . . precedentially largely unsupported . . . [and] has proven unworkable; and, if adopted, it would strengthen the arguments for many other (in my view improper) speech restrictions”); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Privacy Tort*, 68 Cornell L. Rev. 291, 294 (1983) (noting the “serious constitutional problems” with the tort of disclosure of true private facts); *see also* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011) (“This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment.”). [↑](#footnote-ref-179)
180. Ohm, *supra*,at 1129. [↑](#footnote-ref-180)
181. *Id.* [↑](#footnote-ref-181)
182. FTC DATA BROKERS 54. [↑](#footnote-ref-182)
183. Statutory carve out for sensitive data exist in HIPAA and FERPA and others. Regulatory interventions that protect sensitive information include the FTC’s COPPA rule, which includes 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* Ohm, *supra*,at 1134; Heath Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended  in scattered sections of 42 U.S.C.); Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012); 16 C.F.R. §312 (2014) . [↑](#footnote-ref-183)
184. *Id.* 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.”). [↑](#footnote-ref-184)
185. *See, e.g.*, Ohm, *supra* 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 line’s of Google’s definition). [↑](#footnote-ref-185)
186. *See* Ohm, *supra*, at 1138-40. [↑](#footnote-ref-186)
187. *Id.* at 1136. [↑](#footnote-ref-187)
188. *See* Ohm, *supra*, at 1143-44. [↑](#footnote-ref-188)
189. *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/. [↑](#footnote-ref-189)
190. Ohm, *supra*, at 1190. [↑](#footnote-ref-190)
191. *Id.* [↑](#footnote-ref-191)
192. *Id.* at 1192. [↑](#footnote-ref-192)
193. *Id.* at 1192-93. [↑](#footnote-ref-193)
194. *Id.* at 1193. [↑](#footnote-ref-194)
195. *See id.* at 1194; Liane Colonna, *A Taxonomy and Classification of Data Mining,* 16 SMU Sci. & Tech. L. Rev. 309, 332-34 (2013). [↑](#footnote-ref-195)
196. Ohm, *supra*, at1195 (quoting Jeremy Ginsberg et al., *Detecting Influenza Epidemics Using Search Engine Query Data,* 457 Nature 1012, 1013 (2009)). [↑](#footnote-ref-196)
197. 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, 831-2 (2012); Kenneth C. Laudon, *Markets and Privacy*, Comm. Acm (Sept. 1996), at 92, 101. *See generally* Richard R.W. Brooks, *Knowledge in Fiduciary Relations*, in Philosophical Foundations of Fiduciary Law (Andrew S. Gold & Paul B. Miller eds., 2014). [↑](#footnote-ref-197)
198. *See, e.g.*, Eugene Volokh, *Freedom of Speech and 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). [↑](#footnote-ref-198)
199. A major dilemma of much privacy scholarship is how to treat a company’s privacy policy, and to what extent it should function as a contract that binds consumers to (often-unconsidered) agreements and companies to prior promises of privacy. *See, e.g.*, Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 Harv. L. Rev. 1880 (2013); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere),* 87 Notre Dame L. Rev. 1027 (2012); Jeff Sovern, *Opting in, Opting out, Or no Options at all: The Fight For Control Of Personal Information*,74 Wash. L. Rev. 1033 (1999). [↑](#footnote-ref-199)
200. *See* Balkin, *supra*, 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.”). [↑](#footnote-ref-200)
201. *Compare* 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), *with* Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24, 5608-09, para. 25 (defining a broadband internet access service). [↑](#footnote-ref-201)
202. Balkin, *supra*, at 1205. [↑](#footnote-ref-202)
203. *Id.* at 1221; Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age 282 (2015). [↑](#footnote-ref-203)
204. 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, at 1228. [↑](#footnote-ref-204)
205. *See, e.g.*, *id.* at 1187-1194 (Describing a recent Facebook study aimed at manipulating the voting preferences of its users). [↑](#footnote-ref-205)
206. *See* FTC Data Brokers 16-17. [↑](#footnote-ref-206)
207. *See id.* at 17. [↑](#footnote-ref-207)
208. *See supra* Part I. [↑](#footnote-ref-208)
209. *See* Balkin, *supra*, at 1203-1205. [↑](#footnote-ref-209)
210. *See generally* *supra* Parts I & III. [↑](#footnote-ref-210)
211. *See, e.g.*, *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (2010); Fung & Timberg, *supra* (“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.”). [↑](#footnote-ref-211)
212. Dustin Volz, *Email privacy bill unanimously passes U.S. House*, Reuters (Apr. 27, 2016), http://www.reuters.com/article/us-usa-congress-email-idUSKCN0XO1J7. [↑](#footnote-ref-212)
213. *See* 18 U.S.C. § 1702 (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.”) [↑](#footnote-ref-213)
214. Restatement (Second) of Torts § 652 (Am. Law Inst. 1977)(emphasis added). [↑](#footnote-ref-214)
215. *Cf.* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 Yale L. J. Forum 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). [↑](#footnote-ref-215)
216. One exception to this might be the Tor browser, however, even this technology should not be viewed as reliably private, as intelligence and law enforcement agencies will remain in a tug of war over activity that takes place over that or similar browsers. *See supra* Part III. [↑](#footnote-ref-216)
217. *See* United States v. Jones, 132 S.Ct. 945 (2012) (Sotomayor, J., concurring) (underscoring that access to short term GPS data enabled the state to learn when anyone conducted “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). [↑](#footnote-ref-217)
218. 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/ (finding that “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.”). [↑](#footnote-ref-218)
219. FTC Data Brokers 16 (“The data brokers often enter into a variety of written contracts with their data sources. The data brokers may acquire *ownership* of the data under a data supply contract, *use* of the data for a defined time period under a data licensing agreement, or the *right to resell* the source’s product using the data broker’s brand under a data reseller agreement.”). [↑](#footnote-ref-219)
220. Although it remains an open question whether the possibility of tort liability will change the choices of users looking to purchase data on their peers. [↑](#footnote-ref-220)
221. For example, it seems that the plaintiff in the second hypothetical that opens this Note would fail to show that their privacy harm was highly offensive, although courts would likely disagree. On the other hand, a court might reasonably interpret the covert purchase of stolen, highly sensitive information—such as the content of emails or social security numbers—as highly offensive in the intrusion context. [↑](#footnote-ref-221)
222. *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, managments confiscation of an employees 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 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, because he failed to show that his employer invaded his privacy). [↑](#footnote-ref-222)
223. *Id.* at 1138. [↑](#footnote-ref-223)
224. This Note has left unspoken the many benefits of our current data broker regime. Nevertheless they are considerable and require careful weighing of the regulatory interventions this Note proposes. *See, e.g.*, Ohlhausen & Okuliar, *supra*, at 121-124 (describing a broad array of consumer and societal benefits advanced by data availability in the United States). [↑](#footnote-ref-224)
225. *See also* Sebastian Zimmeck, *The Information Privacy Law of Web Applications and Cloud Computing*, 29 Santa Clara Computer & High Tech. L.J. 451 (2013). [↑](#footnote-ref-225)
226. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014). [↑](#footnote-ref-226)
227. *See, e.g.*, Daniel J. Solove, Information Privacy Law 828-835 (5th ed., 2015); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information,* 74 Wash. L. Rev. 1033 (1999). [↑](#footnote-ref-227)
228. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013) (critiquing “privacy self-management” as failing to provide people with meaningful control over their data.) [↑](#footnote-ref-228)
229. Fung & Timberg, *supra* (“‘If the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set,’ said FCC Commissioner Ajit Pai, who suggested that the Federal Trade Commission could accomplish the task.”) [↑](#footnote-ref-229)