Northwestern Journal of International Law & Business

Volume 36
Issue 1 *Winter 2016*

Winter 2016

The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry

Ashley Kuempel

Printed in U.S.A.
Northwestern Journal of International Law & Business
Vol. 36, No. 1

The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry

Ashley Kuempel[*]

Abstract: We live in the era of Big Data, which seeks to commoditize our personal preferences for pecuniary gain. In this changing landscape, data brokers, or information reselling companies, compile information about individuals from a wide range of sources and subsequently sell this information to businesses worldwide. Such practices, however, mostly take place in the shadows without consumers' knowledge or consent, compromising their individual rights to privacy. Further, data brokers often aggregate raw pieces of individual information in a discriminatory manner, leaving consumers vulnerable to predatory and unsavory marketing practices. A 2014 Federal Trade Commission (FTC) Report, Data Brokers: A Call for Transparency and Accountability, specifically addressed such concerns raised by the data broker industry. This Comment analyzes the FTC's findings and demonstrates that the FTC's recommendations, while a step in the right direction, missed the mark on adequate data privacy reform. Rather than taking a piecemeal approach to data privacy in the United States, comprehensive legislation similar to the EU's Data Privacy Directive is necessary to ameliorate the privacy and discrimination concerns facing American consumers today.

* J.D., Northwestern University, 2016; B.A., University of Texas, 2012. The author would like to thank Jefferson Harwell, W. Tyler Perry, and Joe Kim for their valuable feedback. All errors and omissions in this paper remain with the author.

TABLE OF CONTENTS

"[H]e that filches from me my good name
Robs me of that which not enriches him,
And makes me very poor indeed."
—William Shakespeare, *Othello*

INTRODUCTION

Are you a Spanish-speaking Republican smoker who occasionally gambles? Or a diabetic, Catholic single mother who drives a Honda? The data broker industry is currently collecting all of this information and more behind the scenes without your knowledge.[1] Data brokers often know "as much or more about us than our family and friends, including [information about] our online and in-store purchases, our political and religious affiliations, our income and socioeconomic status, and more."[2] Data brokers use "billions of individual data points to produce detailed portraits of virtually every American consumer."[3] As one direct marketer put it, data profiling makes it easy for data brokers to "keep up with the Joneses as well as the Johnsons, the Francos, the Garcias, the Wongs and all the others."[4]

The rise of the data brokers coincided directly with the increase of big data in the marketing sphere.[5] Big data is defined as "high-volume, high-velocity, and/or high-variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization."[6] Though the practice of collecting and selling consumer data to businesses is hardly novel, the unprecedented increase in the volume of data has made it difficult for traditional data processing

---

[1] EDITH RAMIREZ ET AL., FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i (2014), http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter RAMIREZ ET AL., 2014 DATA BROKERS REPORT] (The FTC defined the term "data broker" as a company that "collect[s] consumers' personal information and resell[s] or share[s] that information with others.").

[2] Elizabeth Dwoskin, *FTC Wants More Transparency from Data Brokers*, WALL ST. J. (May 27, 2014, 6:25 PM), http://www.wsj.com/articles/SB10001424052702303903304579588090710049208.

[3] Craig Timberg, *Brokers Use 'Billions' of Data Points to Profile Americans*, WASH. POST (May 27, 2014), http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html.

[4] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 523 (1995) (referring to the discriminatory practices of data brokers described below).

[5] *See* Richard Martinez, *Who's Mining the Store? Big Data Brokers and the Rise of Data Mining*, INSIDE COUNCIL (June 20, 2014), http://www.insidecounsel.com/2014/06/20/whos-mining-the-store-big-data-brokers-and-the-ris.

[6] Michael Matzer, *What Exactly Is Big Data?*, SAP NEWS CENTER (Nov. 20, 2012), http://www.news-sap.com/what-exactly-is-big-data/.

applications to keep up.[7] This is where data brokers come in. As an initial matter, data brokers, or information reselling companies, collect consumer information from a wide variety of sources.[8] They then "extract insight and information from a data set" and "transform it into an understandable structure" for further use in marketing.[9] Data brokers package data by placing consumers into categories, or "buckets,"[10] based on the vast amounts of raw data acquired from online and offline sources alike. They then sell this aggregated data to marketing companies, who use the information to directly target consumers.[11]

A glaring drawback exists in this convenient set up between data brokers and marketing companies—it takes place without consumers' knowledge or consent.[12] Because data brokers operate mostly beyond the gaze of the public eye, individuals are largely unaware of their existence and their monumental impact on day-to-day transactions.[13] This is problematic for two reasons: (1) it invades consumers' rights to privacy and (2) subjects them to unwarranted, and often unforeseeable, discrimination.[14] For one, consumers currently "have no federal statutory right to know what information data brokers have compiled about them for marketing purposes, or even which data brokers hold any such information."[15] Consequentially, "personal information has become a commodity" that is bought and sold by companies "almost entirely at the expense of personal privacy."[16] Further,

---

[7] Ife Adedapo, *Application of big data in business*, PUNCH (Jan. 9, 2015), http://www.punchng.com/business/am-business/application-of-big-data-in-business/ (last visited Sept. 8, 2015).

[8] Commercial sources include, but are not limited to, retailers and catalog companies, magazine publishers, registration websites (such as retail, news, and travel sites), financial service companies, online advertising networks, telephone companies, marketing surveys, warranty registrations, contests, and other data brokers. RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 13–14.

[9] Adedapo, *supra* note 7.

[10] S. COMM. ON COMMERCE, SCI., & TRANSP., OFF. OF OVERSIGHT AND INVESTIGATIONS MAJORITY STAFF, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES i (2013) (report for Senator Rockefeller, Chairman, S. Comm. On Commerce, Sci., & Transp.), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

[11] *Id.* at 12.

[12] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at vii; *see, e.g.,* Cynthia Alice Andrews, *Breaking It Down: The Data On Data Brokers*, FLIPTHEMEDIA (Feb. 9, 2015), http://flipthemedia.com/2015/02/breaking-data-data-brokers/ (describing how data brokers purchase consumer data, such as payment methods, types of purchases, and the like, from commercial sources without consumer knowledge).

[13] *See* RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, app. C-1 (concurring statement of Commissioner Julie Brill at C-1).

[14] *See* RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 46–47 (explaining how data brokers combine and analyze data about consumers to "make inferences about them, including potentially sensitive inferences.").

[15] S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 3.

[16] ANN CAVOUKIAN, ONTARIO INFORMATION AND PRIVACY COMMISSIONER, PRIVACY AS A

and perhaps most importantly, placing consumers in "buckets" allows marketing companies to discriminate against individuals and subject them to unequal access to information, differential pricing, and predatory practices.[17] Thus, while data brokers and marketing companies prosper,[18] consumers are continuously hurt by this "vogue for data."[19] In the words of FTC Commissioner Julie Brill, data broker profiles "have the ability to not only rob us of our good name, but also to lead to lost economic opportunities, higher costs and other significant harm."[20]

A 2014 Federal Trade Commission (FTC) report, *Data Brokers: A Call for Transparency and Accountability* (FTC Report), attempted to "lift [this] veil of secrecy . . . shroud[ing] the data broker industry."[21] The FTC performed a study of nine data brokers representing a cross-section of the industry, which included over 1,000 companies.[22] The FTC Report focused on three products data brokers create: (1) marketing products, (2) risk mitigation products, and (3) people search products.[23] This Comment will focus on the FTC's legislative recommendations regarding marketing products alone.

The FTC Report's conclusions, which include the privacy and discrimination concerns discussed above, should give Congress a "powerful and disturbing wake up call."[24] Though Congress has addressed data

---

FUNDAMENTAL HUMAN RIGHT VS. AN ECONOMIC RIGHT: AN ATTEMPT AT CONCILIATION i (1999).

[17] *See* S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 6–7.

[18] In 2012, the data broker industry generated $150 billion in revenue, which is twice the size of the entire intelligence budget of the U.S. government. Matt Kapko, *Inside the Shadowy World of Data Brokers*, CIO (Mar. 27, 2014, 8:00 AM) http://www.cio.com/article/2377591/data-management/inside-the-shadowy-world-of-data-brokers.html (In a statement to members of Congress, Digital Marketing Association claimed that in the digital age, "data-driven marketing has become the fuel on which America's free market engine runs.").

[19] Konstantin Kakaes, *The big dangers of 'big data,'* CNN (Feb. 4, 2015, 12:11 PM), http://www.cnn.com/2015/02/02/opinion/kakaes-big-data/index.html.

[20] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, app. C-1 (concurring statement of Commissioner Julie Brill at C-3); *see also, id.* at vi (describing how data brokers have the potential to rob consumers of economic opportunities) ("For example, while a data broker could infer that a consumer belongs in a data segment for 'Biker Enthusiasts,' which would allow a motorcycle dealership to offer the consumer coupons, an insurance company using the same segment might infer that the consumer engages in risky behavior.").

[21] Sam Pfeifle, *Industry Reaction to FTC Data Broker Report: Eh.*, THE PRIVACY ADVISOR (May 28, 2014), https://privacyassociation.org/news/a/industry-reaction-to-ftc-data-brokers-report-eh/ (statement by FTC Commissioner Edith Ramirez).

[22] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at i; Though the FTC's general role is to investigate certain practices and make legislative recommendations, it also has the power to declare data broker practices "unlawful" should they constitute "unfair or deceptive acts." 15 U.S.C. § 45(a)(1) (1982). The FTC, however, did not declare data brokers "unlawful" in its report.

[23] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at i.

[24] Steve Lohr, *New Curbs Sought on the Personal Data Industry,* N. Y. TIMES (May 27, 2014), http://www.nytimes.com/2014/05/28/technology/ftc-urges-legislation-to-shed-more-light-on-data-collection.html?_r=0 (statement by Jeffrey Chester, executive director of the Center for Digital

privacy in certain sectors, no all-encompassing data privacy legislation exists to protect consumers from data brokers in the marketing realm.[25] The FTC made several legislative recommendations in the FTC Report, most of which aimed to increase the transparency of data brokers.[26] Such proposals included (1) creating a centralized Internet portal in which data brokers identify themselves,[27] (2) mandating disclosure requirements regarding data brokers' use of aggregated data,[28] and (3) increasing transparency regarding the sources of data brokers.[29]

The FTC's proposals, however, missed the mark—they lacked adequate individual protections in a world where the consumer "is not the customer, but the product."[30] Congress should strive for a more comprehensive approach similar to the European Union's Data Privacy Directive (Data Directive) in order to adequately improve consumer rights in the big data industry.[31] This Comment will examine the dire effects of big data practices on American consumers and the need for legislation similar to the Data Directive. Due to the considerable differences between the United States and the EU's approach to privacy[32] and the different historical bases underlying these approaches,[33] it is unrealistic to expect Congress to replicate the Data Directive on its first try.[34] Rather, this

---

Democracy).

[25] Ieuan Jolly, *Data Protection in United States: Overview*, PRACTICAL LAW (July 1, 2015), http://us.practicallaw.com/6-502-0467#null.

[26] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 49–53.

[27] *Id.* at 52.

[28] *Id.*

[29] *Id.*

[30] Lohr, *supra* note 24 (statement by Marc Rotenberg, Executive Director of the Electronic Privacy Information Center).

[31] *See* Jennifer M. Myers, *Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States,* 29 CASE W. RES. J. INT'L L. 109, 114 (1997) ("The United States should adopt comprehensive data legislation immediately.").

[32] "Principally, there are two main approaches to protecting an individuals 'right' of privacy: legislation and self-regulation, with the Europeans [favoring] the former and the Americans inclined towards the latter." CAVOUKIAN, *supra* note 16, at i; *see also* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 196 (1999) ("When compared with the omnibus, centralized data protection of the EU directive and member states' national laws, U.S. privacy protection stands in stark contrast and to some observers seems to pale altogether.").

[33] DONALD C. DOWLING, JR., WHITE & CASE, INTERNATIONAL DATA PROTECTION AND PRIVACY LAW 4 (2009), http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf ("Nefarious uses of secret files under World War II-era fascists and post-War Communists instilled in many Europeans an acute fear of the unfettered abuse of personal information—a fear that lingers to this day. . . . This is a cultural issue different for frontier-spirited Americans to understand . . . .").

[34] Data privacy laws are inextricably linked to the cultural and social norms of the countries from which they emerge. The United States and Europe, while similar to some extent, vary considerably in

Comment argues that the United States should adopt the Data Directive's specific individual safeguards in order to protect consumers from data brokers. The ample privacy and discrimination concerns emerging from big data practices outweigh the benefits of direct marketing in the private sector. As such, adequate legislation should include, at a minimum, the same provisions from the Data Directive that ensure that the burden of protecting consumers falls on the data collectors, rather than the consumers themselves.[35] Though revamping the U.S. data privacy regime could impose significant burdens on marketing companies,[36] such reform is necessary to ameliorate the rights of American individuals.

In order to examine the thesis laid out in the preceding paragraph, this Comment will proceed as follows. Part I of this Comment will address the current data privacy framework in the United States and the privacy and discrimination concerns it presents to consumers.[37] Part II of this Comment will explain why each of the legislative recommendations made by the FTC Report does not adequately protect American consumers. In Part III, this Comment will demonstrate why certain provisions within the EU's Data Directive should be used as a model for future U.S. data broker legislation. Finally, the Conclusion will offer solutions. Ultimately, the potential harm to consumers outweighs the benefits of big data, and Congress should err on the side of overprotection by passing legislation in line with the Data Directive.

I. DATA PRIVACY IN THE UNITED STATES

A. U.S. Sectoral Approach

According to Samuel Warren and Louis Brandeis, "the right to life . . . [means] the right to enjoy life—the right to be let alone."[38] Data brokers in

---

their social, political, and historical backdrops. *See* Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2),* 18 INT'L J.L. & INFO. TECH. 227, 243 (2010) ("Data protection law around the world is based on divergent cultural and legal values."); *see also* DOWLING, JR., *supra* note 33, at 4.

[35] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Data Directive]; Section IV, Article II of the Directive requires that upon data collection, a controller must "inform the data subject of the controller's identity and its purpose for processing the data." Consumers also have the right to have inaccurate data rectified and can withhold person information in certain circumstances. *E.g.*, *id.* § IV, art. II.

[36] *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 18 (2000).

[37] *Id.*

[38] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 n.1 (1890) (Warren and Brandeis' revolutionary law review advocated for the existence of an implicit right to privacy, claiming that "the elasticity of our law, its adaptability to new conditions, the capacity for growth, which has enabled [our law] to meet the wants of an ever changing society and to apply

the private sector, however, continually deprive American consumers of this right. In the United States, no generalized protection exists to shield consumers from the processing of their personal information by the private sector.[39] For one, there is no explicit right to privacy in the Constitution.[40] The Supreme Court has only recognized the implied right to privacy with respect to "intrusive government activities,"[41] not to safeguard individuals from the private sector. Because this Constitutional common law solely focuses on the public sector, it provides little to no protection in a world where "big business is the real Big Brother."[42] And as the FTC Report pointed out, in today's economy, "Big Data is big business."[43]

Further, no comprehensive legislation exists in the United States regarding data privacy.[44] Congress employs a "sectoral approach" to data collection, enacting a series of unconnected laws targeting specific markets.[45] For example, Congress regulates particular categories of data, such as financial or health information,[46] but leaves data collection in the marketing sphere largely unregulated.[47] This "patchwork system" of federal

immediate relief for every recognized wrong, have been its greatest boast."); Joel E. Smith, *Invasion of Privacy by Sale or Rental List of Customers, Subscribers, or the Like, to One Who Will Use it for Advertising Purposes,* 82 A.L.R.3d 772 (1978) ("[I]t was not until the publication in 1890 of a law review article by Warren and Brandeis that the right [to privacy] was introduced and defined as an independent right and the distinctive principles upon which it is based were formulated.").

[39] *See* Shaffer, *supra* note 36, at 24.

[40] Though the Bill of Rights arguably protects specific aspects of privacy, there is no express right to privacy in the Constitution. *See, e.g.* U.S. CONST. amend. I (protects the privacy of beliefs); U.S. CONST. amend. IV (privacy of the person and his possessions against unreasonable searches and seizures).

[41] *See* Cate, *supra* note 32, at 196; *see, e.g.,* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that federal authorities' use of an electronic listening device outside of a telephone booth used by the plaintiff was unconstitutional under the Fourth Amendment); *see also* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (standing for the proposition that specific guarantees in the Bill of Rights have "penumbras" which encompass an individual's right to make personal decisions free from government intrusion).

[42] CAVOUKIAN, *supra* note 16, at 1 (statement by Ann Wells Branscomb, a highly respected privacy scholar).

[43] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at i.

[44] Jolly, *supra* note 25.

[45] Amanda C. Border, *Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States,* 35 SUFFOLK TRANSNAT'L L. REV 363, 364–65 (2012).

[46] Jolly, *supra* note 25 (citing the following examples of sector-specific regulatory laws: (1) the Gramm-Leach-Bliley Act (GLB), which regulates the collection, use, and disclosure of financial information; (2) The Health Insurance Portability and Accountability Act (HIPAA), which regulates medical information; and the Fair Credit Reporting Act (FCRA), which applies to consumer reporting agencies).

[47] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at i; JOHN IRONS & ISAAC SHAPIRO, REGULATION, EMPLOYMENT, AND THE ECONOMY, ECONOMIC POLICY INSTITUTE (2011), http://www.epi.org/publication/regulation_employment_and_the_economy_fears_of_job_loss_are_over blown/ (Members of Congress justify deregulation on the grounds that "regulations raise cost for firms, thereby raising the costs of products, thereby leading to a reduction in sales and employment.").

and state laws often involves regulations that "overlap, dovetail, and contradict one another," making it difficult for an individual to protect his or her privacy.[48]

Congress's approach to data use and collection is based in part on the prevailing attitude that the privacy of personal data is an "economic issue rather than a fundamental right."[49] In the United States, personal information is frequently seen as a commodity that can be traded for goods and services.[50] An assumption inherent in this market-based approach is that companies "have a legitimate interest in acquiring personal information for business purposes, and this should not be arbitrarily restricted [by privacy concerns]."[51] Industry representatives argue that an "overly broad, prescriptive, one-size-fits-all [legislative] approach would hinder or undermine the ability of companies to innovate in a global economy."[52] Consequentially, rather than adopting the Warren/Brandeis framework,[53] Americans view data privacy as one interest to be balanced against many others, treating it as secondary to other concerns.[54] As such, an individual's interest in privacy is often superseded by the interest in a business's ability to acquire personal information.[55] The issue with this commodification of data is that it lacks corresponding privacy protections for consumers, allowing companies to reign free without providing consumers with compensation, notice, or choice.[56]

As a result of these underlying philosophies, Congress tends to respond reactively, rather than proactively, when addressing data privacy concerns.[57] For instance, the Fair Credit Reporting Act (FCRA), which

---

[48] Jolly, *supra* note 25; *see also* CAVOUKIAN, *supra* note 16, at 5 ("From the individual's perspective, this patchwork of laws leaves a fragmented legal terrain that burdens, and possibly overwhelms, an individual's ability to protect his or her privacy.").

[49] Morey Elizabeth Barnes, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171, 175 (2006); *see also* RONALD B. STANDLER, FUNDAMENTAL RIGHTS UNDER PRIVACY IN THE USA (2012), www.rbs2.com/priv2.pdf (demonstrating that the right to individual data does not qualify as a fundamental right) ("There are only a few fundamental rights that have been recognized by the U.S. Supreme Court under the classification of *privacy* [such as rearing children, procreation, marriage, and family].").

[50] CAVOUKIAN, *supra* note 16, at iv.

[51] CAVOUKIAN, *supra* note 16, at 14.

[52] Natasha Singer, *Data Protection Laws, an Ocean Apart,* N. Y. TIMES (Feb. 2, 2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?_r=0 (statement by Kevin Richards, Senior Vice President of Federal Government Affairs at TechAmerica).

[53] Smith, *supra* note 38.

[54] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 880 (2013).

[55] CAVOUKIAN, *supra* note 16, at 14.

[56] *Id.* ("[P]ersonal information now has some of the characteristics of a 'public good,' and, as such, is widely available.").

[57] Border, *supra* note 45, at 364–65.

regulates the use of individual data by consumer credit reporting agencies, was enacted in reaction to the "consumer horror stories of dealings with credit reporting agencies."[58] The Driver's Privacy Protection Act (DPPA), which governs the dissemination of information obtained by the Department of Motor Vehicles, was a response to the "murder of an actress . . . who was tailed by a stalker who obtained her address . . . from state driver's license records."[59] Further, the Video Privacy Protection Act (VPPA), passed in 1988, regulates the disclosure of tape rental or sale records.[60] It was passed shortly after the video records of Judge Robert Bork were obtained and used by a news reporter in a campaign against his Supreme Court nomination.[61] This reactive, sectoral legislative approach creates considerable inconsistencies in U.S. data privacy laws, leaving numerous sectors unregulated and considerable amounts of personal information unprotected.[62]

B. The Implications of Self-Regulation

Because data brokers in the marketing industry are currently unregulated by data privacy legislation, they are controlled exclusively by self-regulation, which is defined as "self-created privacy standards based on the industry norm."[63] Industry trade associations, for example, have identified voluntary "best practice guidelines for [their] members."[64] Such recommendations include the Direct Marketing Association's "Guidelines for Ethical Business Practice," which contain recommendations on handling and protecting consumer information.[65] Proponents of self-regulation argue that comprehensive legislation is too inflexible and time-dependent to keep up with the "fast-moving world of information technology."[66] Further, self-regulation is seen as less bureaucratic and costly than abiding by federal restrictions.[67]

---

[58] Shaffer, *supra* note 36, at 25.

[59] *Id.*

[60] 18 U.S.C. § 2710 (1988).

[61] Shaffer, *supra* note 36, at 25.

[62] Jolly, *supra* note 25 ("Some [existing federal privacy laws] apply to particular categories of information, such as financial or health information, or electronic communications. Others apply to activities that use personal information, such as telemarketing or commercial e-mail."). However, personal information used for marketing purposes is largely unregulated. *See* Schwartz & Solove, *supra* note 54, at 880.

[63] Border, *supra* note 45, at 367–78; *see also* CAVOUKIAN, *supra* note 16, at 10 ("Self-regulation, as understood, means that a given business or industry sector establishes privacy rules among the firms that make up that sector.").

[64] S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 4.

[65] DIRECT MARKETING ASSOCIATION, DIRECT MARKETING ASSOCIATION GUIDELINES FOR ETHICAL BUSINESS PRACTICE 2 (2011).

[66] CAVOUKIAN, *supra* note 16, at 8.

[67] CAVOUKIAN, *supra* note 16, at 8–9 ("It is feared that government legislation will likely lead to an

But is self-regulation truly a substitute for comprehensive legislation?[68] Unfortunately for the data broker industry, the answer is unequivocally no. For one, self-regulation is voluntary, meaning that the industry "can[not] discipline outliers who do not play by the rules."[69] Consequentially, some companies abide by self-regulation while others do not, resulting in a fragmented and disparate system of privacy rules.[70] In a Senate Judiciary Committee investigation, for example, the Committee found that respondent companies' voluntary policies varied widely regarding consumer access and correction rights concerning consumers' own data.[71] This lack of uniformity is also largely due to the absence of another key component necessary for effective regulation: enforcement.[72] Though the FTC treats violations of a company's own privacy policy as a "deceptive business practice," it cannot touch companies who refuse to put up privacy policies in the first place.[73] Moreover, FTC enforcement is "'sporadic' at best."[74] As of 2009, for example, the FTC had only listed twenty-five enforcement actions of this nature,[75] undoubtedly leaving many companies free from regulation.

Further, even when companies decide to "comply" with the industry norm, privacy experts argue that they put up smoke screens in place of legitimate privacy protections.[76] Data brokers' privacy policies, for example, appear to contain numerous provisions regarding individual rights

---

overly bureaucratic and cumbersome regulatory process that will only result in raising the operating costs of the businesses involved.").

[68] Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?,* THE PRIVACY ADVISOR (Jun. 24 2014), https://privacyassociation.org/news/a/will-industry-self-regulation-be-privacys-way-forward (statement by Sally Greenberg, National Consumer League Executive Director) (*"*We are supporters of self-regulation as an industry practice but never as a substitute for the rule of law. Appropriate laws and regulations are necessary to ensure that all players have to abide by the same rule.").

[69] *Id.* (statement by Sally Greenberg, National Consumer League Executive Director).

[70] The director of the SEC, for example, testified before Congress in 2008, stating, "We have learned that voluntary regulation does not work. . . . The lessons of the credit crisis all point to the need for strong and effective regulation." IRONS & SHAPIRO, *supra* note 47; CAVOUKIAN, *supra* note 16, at 9.

[71] Some companies have virtually no rights in their policies, while others, such as Acxiom, have more fulsome policies that allow for consumer access and correction. S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at iii.

[72] Richard M. Marsh Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 MICH. TELECOMM. & TECH. L. REV. 543, 555 (2009).

[73] *Id.*

[74] *Id.*; *see also* Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 156 (2006) (describing the justification behind the FTC's sporadic approach to enforcement) ("[F]TC enforcement actions tend to focus on heavy-weight companies that bring in headlines and settlements for the government. Thus, for example, in its few enforcement actions, the FTC has gone after companies such as Geocities, Equifax, Experian, Hersey Foods, Mrs. Field's, and Quicken Loans.").

[75] Marsh Jr., *supra* note 72, at 555.

[76] *See* Shaffer, *supra* note 36, at 27.

but actually reveal little to no information.[77] These policies are often unintelligible, "full of electronic boilerplate," and "often includ[e] a clause that reserves the company the right to change their data standards at any time."[78] Thus, "these 'self-regulatory schemes' remain voluntary, unenforceable, and . . . often ignored by the very companies advocating their use."[79]

C. The FTC Report

The FTC Report, which discussed the results of an in-depth study of nine data brokers, weighed the costs and benefits of big data in the marketing sector.[80] According to the FTC, consumers benefit from data brokers' collection and usage of their personal data.[81] Such "benefits" include easier access to goods and services and increased innovative product offerings from a wider range of businesses.[82] By acknowledging these advantages, the FTC added fuel to the central claim of data proponents that data always has some positive value.[83] This premise, however, is false.[84] The FTC should have used this opportunity to focus solely on the risks of the big data industry rather than watering down the negative effects of data broker practices with these so-called "advantages."

The FTC Report, however, did not completely drop the ball. It effectively addressed two major issues with data broker practices explained in detail below: (1) the fundamental lack of transparency of data brokers,[85] and (2) the "aggregation effect" of transforming raw data into insensitive, discriminatory categorizations.[86]

1. A Fundamental Lack of Transparency Equals Privacy Infringement

According to the FTC, a "fundamental lack of transparency" exists behind data brokers' practices.[87] Data brokers collect consumer information from a wide-range of online and offline sources without the consumer's

---

[77] Marsh Jr., *supra* note 72, at 554.

[78] *Id.* (citing Wayne B. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1604 (2006)).

[79] Shaffer, *supra* note 36, at 27.

[80] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at i.

[81] *Id*. at 47–48.

[82] *Id*.

[83] Kakaes, *supra* note 19.

[84] *Id*.

[85] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at vii.

[86] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1889–90 (2013).

[87] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1 at vii.

knowledge or consent.[88] To further complicate the matter, data brokers purchase individual data from one another, creating an intricate web of information sharing that is nearly impossible for consumers to trace.[89]

Though individuals often provide consumer-facing sources with information willingly, they are largely unaware that this information is then provided to data brokers in a different context for a different purpose.[90] For instance, according to a recent study, "64% [of . . . people surveyed] do not know that a supermarket is allowed to sell other companies information about what [consumers] buy."[91] As a result, it is more likely than not that a simple purchase of Kashi cereal at the grocery store will place you in the "New Age/Organic Lifestyle" bucket in some data broker's database.[92] Thus, data from even the simplest of consumer transactions can be bought, manipulated, and sold on the big data marketplace.[93]

Even more troubling is the possibility that consumers who register on medical websites sometimes find their personal information entangled in a web of big data.[94] This is particularly detrimental when the medical website is affiliated with sensitive conditions such as AIDS, diabetes, or depression. The FTC Report affirmed that some data brokers "sell marketing lists identifying consumers who have addictions, AIDS, HIV, [and] genetic diseases."[95] Data brokers are thus essentially "panning for gold"[96] in consumers' private matters for profit. In the words of FTC Commissioner Julie Brill who summed up such danger, "[w]hat damage is done to our individual sense of privacy and autonomy in a society in which information about some of the most sensitive aspects of our lives are available for analysts to examine . . . and for anyone to buy if they are willing to pay the going price?"[97]

2. The Aggregation Effect: With Distortion Comes Discrimination

Most importantly, rather than merely collecting individual pieces of

---

[88] *Id.* at vii.

[89] *Id.* at 51.

[90] *Id.* at 55 (The Commission voiced concerns about this issue numerous times, advocating that data brokers "take reasonable precautions to ensure that downstream users of their data do not use it for eligibility discriminations or for unlawful discriminatory purposes.").

[91] Solove, *supra* note 86, at 1886 (2013).

[92] *See* RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 21.

[93] *See id.* app. C-1 (concurring statement of Commissioner Julie Brill at C-4).

[94] *See id.*

[95] *See* RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 25 n.57.

[96] Matt Kapko, *supra* note 18 ("Those who are aware should be shocked by the extent to which their online and offline behaviors are being sifted through for profit. Call it panning for gold in the digital age.").

[97] Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at the 23rd Computers Freedom and Privacy Conference, Reclaim Your Name (June 26, 2013).

raw data, data-collecting companies use learning algorithms to make inferences about consumers, placing them in categories related to ethnicity, income, religion, and political affiliations.[98] After collecting raw data from a multitude of sources, data brokers merge this data, creating a "detailed composite" of the consumer's life.[99] This is called the "aggregation effect."[100] Proponents of the aggregation effect claim that these detailed personal profiles are "effective in the consumer marketplace and can deliver products and offers to precise segments of the population."[101] They argue that big data algorithms allow consumers to make purchase decisions based on their prior interests[102] rather than starting from scratch. What they fail to note, however, is that many of these "detailed composites" are insensitive and serve as vehicles for discrimination.[103] Many attempts to collect and aggregate data not only miss key factors, but transform for the worse the systems they claim to be measuring.[104] According to the FTC, data brokers' marketing products may facilitate the direct marketing of "health, ethnicity, or financial products," which could trouble consumers and "undermine their trust in the marketplace."[105]

After collecting millions of data points from copious sources on a particular individual, data brokers place that consumer in "buckets" or categories designed to facilitate direct marketing.[106] These buckets are the tools in which marketing companies target, exclude, and prey on individual consumers. For instance, data brokers who categorize consumers by their ethnicity or financial situation make it easier for rapacious businesses to prey on them or subject them to differential pricing.[107] Categories such as "Urban Scramble,"[108] which describes consumers of largely African

---

[98] *See* RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 19 ("In developing their products, the data brokers use not only the raw data they obtain from their sources, such as a person's name, address, home ownership status, age, income range, or ethnicity . . . but they also derive additional data.").

[99] *See* RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 46.

[100] Solove, *supra* note 86, at 1890 (2013).

[101] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES PRESERVING VALUES 7 (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf [hereinafter WHITE HOUSE REPORT].

[102] Jonathan Shaw, *Why "Big Data" Is a Big Deal*, HARV. MAG. (Mar.–Apr. 2014), http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal.

[103] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 20 n.52.

[104] Kakaes, *supra* note 19.

[105] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 48.

[106] S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 6.

[107] *Id.* at ii. It is important to note that, while FTC enforcement has been sporadic, the FTC has fined some companies for such unscrupulous activities. For example, in 2011, Teletrack, Inc., a data broker, sold lists of consumers who had previously applied for non-traditional credit products to third parties, primarily payday lenders and sub-prime auto lenders, that wanted to use the information to target consumers. The FTC charged Teletrack with a $1.8 million penalty as a result. *See id.* at 7.

[108] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 47.

American and Latino descent with low incomes, attract companies specializing in high-cost loans or financially-risky products who are looking to target populations likely to "need quick cash."[109] Moreover, data brokers have developed marketing tools to assist companies in "identify[ing] and effectively market[ing] to under-banked consumers," which include "new legal immigrants, recent graduates, widows" and "consumers with transitory lifestyles, such as military personnel" who spend millions annually on payday loans and other "non-traditional" financial products.[110] Though categories such as "Financially Challenged" or "Underbanked" may "implicate creditworthiness," the use of data about a consumer's financial status for marketing purposes is generally not covered by the FRCA, unless the marketing is for certain pre-approved offers of credit.[111]

A specific example of these discriminatory practices warrants attention. In 2007, InfoUSA, a data broker, sold lists of elderly consumers to individuals who used the lists to target senior citizens with fraudulent sales pitches.[112] InfoUSA aggregated individual data and subsequently advertised lists of "Suffering Seniors," people with cancer or Alzheimer's disease, "Oldies but Goodies," people over 55 who liked to gamble, and "Elderly Opportunity Seekers," older people "looking for ways to make money."[113] One category explicitly said, "[t]hese people are gullible. They want to believe that their luck can change."[114] This "bucketing" of consumer data allowed telemarketers to purchase this information and trick vulnerable senior citizens into revealing their bank information in order to raid their accounts.[115] Though the FTC Report did not investigate InfoUSA in particular, this example illustrates the risks raised by buckets identifying financially and physically vulnerable consumers.[116]

3. A Lack of Consumer Redress

Consumers have little redress to ameliorate the privacy and discrimination concerns raised by big data. For one, as discussed above, consumers' federal statutory rights in the marketing realm are basically

---

[109] Other insensitive categories related to ethnicity and financial status include: "Ethnic Second-City Strugglers," "Rural and Barely Making It," "X-tra Needy," "Small Town Shallow Pockets" and "Credit-Crunched: City Families." S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 24–25.

[110] *Id*. at 25.

[111] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 25 n.58.

[112] Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N. Y. TIMES, May 20, 2007, http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=0.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *See* S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 26.

nonexistent.[117] Further, with the exception of information for pre-screened offers of credit or insurance, consumers do not have the right to control what personal information about them is collected and shared, even where such information concerns sensitive matters.[118] Consumers also lack a statutory right to correct data inaccuracies.[119]

Further, consumers are largely unaware of data brokers' existence in the first place.[120] Consequentially, "to the extent that some data brokers offer consumers the ability to correct or suppress their data, consumers [do not] know [of] these rights, rendering [them] illusory."[121] Even consumers who visit data broker websites are not given the whole picture. On their websites, data brokers generally provide access to raw data—age, name, and birthplace—while failing to disclose more problematic algorithm-based inferences such as "Urban Scramble," leaving consumers largely in the dark.[122] Simply seeing that a data broker knows that you are single between the ages of fifty and seventy-five is no cause for alarm. Seeing that a data broker has tagged you as an "older, down-scale and ethnically-diverse single" typically "between the ages of 50 and 75" who is part of the "underclass of the working poor and destitute seniors without family support,"[123] however, is a completely different story.

On the rare occasion that consumers actually gain access to information they wish to suppress, they are usually confronted with ambiguous and technical opt-out choices.[124] Most consumers are unaware that, in the world of big data, "opt-out" is *not* synonymous with delete.[125] Instead, opt-out means "suppressing the consumer's personal information from display in the data broker's marketing products" while still keeping the information in the database.[126] As a result, some data brokers continue to use suppressed information "in products that display data in an anonymous, aggregated form" rather than ceasing use altogether.[127] "Opting out" of data use therefore does not relieve consumers of the privacy burdens

[117] No federal law gives consumers the right "to know what information data brokers have compiled about them for marketing purposes, or even which data brokers hold such information." *Id.* at 3.

[118] *Id*.; While there is legislation pending in Congress aimed at improving the transparency behind data broker practices, such legislation fails to adequately address the privacy and discrimination concerns posed by data brokers. *See, e.g.*, Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014), https://www.congress.gov/113/bills/s2025/BILLS-113s2025is.pdf (Act introduced by Senators Jay Rockfeller and Ed Markey).

[119] S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 3.

[120] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at C-3 (concurring statement of Commissioner Julie Brill at app. C-1).

[121] *Id.*

[122] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 42.

[123] S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 25.

[124] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 49.

[125] *Id.*

[126] *Id.* at 42–43.

[127] *Id.* at 43.

of big data—their information is still in the system regardless of their attempts to suppress it.

In sum, the choices available to consumers, to the extent that they even exist, are mostly "invisible or incomplete."[128] Most of these choices are available *ex post*, providing consumers only with limited options after their data has been bought, aggregated, and sold.[129] As a result, legislation should be enacted to impose *ex ante* regulations on data brokers, providing consumers with adequate safeguards before collection even takes place.[130]

II. THE FTC'S LEGISLATIVE RECOMMENDATIONS: A MISSED OPPORTUNITY FOR ADEQUATE REFORM

The FTC recommended several pathways for Congress to remedy the "fundamental lack of transparency" surrounding data brokers in the United States.[131] In light of its findings, the FTC suggested that Congress consider enacting legislation that would "enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information . . . held by these entities."[132] Specifically, the Commission suggested Congress pass laws that would allow consumers to: (a) access their data, and (b) opt-out of having their personal information distributed for marketing purposes.[133]

The FTC's recommendations, though undoubtedly a step in the right direction, illustrated a "missed opportunity" to take a harder stance on data privacy rights.[134] The recommendations place the majority of responsibility on the consumer to mitigate privacy and discrimination issues they may not even be aware of, adhering to the "same old privacy self-management model" that has crashed and burned in the past.[135] Rather than protecting consumers from abusive practices, the legislative goals of the FTC force individuals to retroactively engage in damage control by making them search for their data and attempt to "opt-out" of its use. The FTC Report therefore focuses too exclusively on individual choice and not enough on the regulation of the big data industry itself.[136]

---

[128] *Id.* at 49.

[129] *See* Solove, *supra* note 86, at 1894 (describing the ex post, privacy self-management regime in the United States).

[130] This would be a considerable change from the privacy self-management framework running rampant through the United States, and would ameliorate the bargaining position of individual consumers significantly. *See generally id*.

[131] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at vii.

[132] *Id.* at 49.

[133] *Id.* at 50.

[134] Lohr, *supra* note 24 (statement by Marc Rotenberg, Executive Director of the Electronic Privacy Information Center).

[135] Solove, *supra* note 86, at 1883.

[136] *See id*. at 1893.

A. The Centralized Portal

As an initial matter, the FTC suggested that Congress require data brokers to create a centralized Internet portal in which they identify themselves, describe their practices, and allow consumers to access their data at a "reasonable level of detail."[137] According to the FTC, Congress could enact legislation requiring consumer-facing sources to give notice that they share data with data brokers and to provide consumers with a link to the centralized portal.[138] These sources would also have to give consumers the ability to opt-out or suppress data upfront.[139]

Though the creation of such a centralized portal would increase transparency to a certain extent, it would not be an effective safeguard for consumers in an increasingly data-driven world.[140] Such legislation would fail to provide adequate consumer redress for the following reasons. First, the FTC recommended that Congress only require a group of around fifty of the largest data brokers to participate.[141] While this would shed some light on the practices of the most dominant players in the data-collection industry, it would leave the majority of private companies unchecked.[142] FTC Commissioner Josh Wright voiced similar concerns about the effectiveness of the portal, stating that the fifty largest data brokers "might be the ones with the most consumer-friendly practices," leaving the smaller ones that "specialize in collecting and using more sensitive information" unchecked.[143] For instance, Julia Angwin, an investigative journalist, found 212 data brokers with her personal information after a month of trying to opt-out of data brokers' websites.[144] Angwin's personal experience highlights the fact that disclosing the practices of a mere fifty data brokers

[137] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 50–51.

[138] *Id.* at 52.

[139] *Id.*

[140] *See* Kapko, *supra* note 18 ("Data brokers are becoming increasingly important because. . . . [they] enhance the targeting efficiency [of marketing companies] by leveraging consumer data.") (citation omitted); *see also* Adedapo, *supra* note 7 ("63 per cent of global businesses use analytics in creating [a] competitive advantage for their organisations.").

[141] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 51.

[142] *Id.*; *see also Online List of Data Brokers*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/online-information-brokers-list (last visited Sept. 11, 2015) (this website posted a non-exhaustive 270 data brokers, which indicates that fifty participants do not constitute as a majority).

[143] Christopher Wolf, *The Hidden Mini Dissents in the Data Broker Report of Federal Trade Commissioner Wright,* THE PRIVACY ADVISOR (July 31, 2014), https://privacyassociation.org/news/a/the-hidden-mini-dissents-in-the-data-broker-report-of-federal-trade-commissioner-wright/.

[144] Julia Angwin, *Privacy Tools: Opting Out from Data Brokers*, PROPUBLICA (Jan. 30, 2014, 12:29 PM), http://www.propublica.org/article/privacy-tools-opting-out-from-data-brokers.

would not effectively remedy the extreme discrimination concerns facing individuals.[145]

Second, such legislation would only require that data brokers on the portal allow consumers access to information at a "reasonable level of detail," and that they disclose any information that they deem "sensitive."[146] This allows data brokers to reveal only a sliver of the extensive amount of data in their possession, providing them with the same self-regulation accepted in the past. Though this recommendation would regulate data brokers to the extent that it compels them to disclose "sensitive" data, this is a largely subjective requirement. In fact, the FTC itself acknowledged that what qualifies as sensitive often lies in the eye of the beholder.[147] By recommending that data brokers should include "categories that some consumers might find sensitive and others may not,"[148] the FTC failed to draw any semblance of a line.[149] While certain data, such as whether a consumer has AIDS, would qualify as sensitive across the board,[150] other categories are not so straightforward. Labels regarding one's ethnicity or financial status,[151] for instance, may not be deemed subjectively sensitive enough to pass the threshold.

Even assuming data brokers, courts, and/or agencies will err on the side of an overbroad classification of sensitive information, this suggestion fails to address the main vehicle for discrimination in the data broker industry: consumer bucketing via data aggregation.[152] Though the disclosure of potentially sensitive raw data would put consumers on alert of discrimination to a certain extent, many sensitive buckets arising from aggregation, such as "Urban Scramble,"[153] could be left out of the portal. Thus, the limited amount of data brokers required to participate in the portal, combined with the wide discretion of data brokers regarding what they disclose, renders this suggestion inadequate. Legislation is needed to

---

[145] *See, e.g.*, Duhigg, *supra* note 112 (exemplifying how data brokers can discriminate against and take advantage of the elderly).

[146] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 51.

[147] *Id.*

[148] *Id.*

[149] For an example of a better-defined line regarding what constitutes as "sensitive," see Data Directive, *supra* note 35, art. 8(1).

[150] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 51.

[151] For example, a consumer labeled by brokers as "Financially Challenged," which describes single parents in their "prime working years" who are "struggl[ing] with some of the lowest incomes" and are "[n]ot particularly loyal to any one financial institution," might find this label offensive or overtly sensitive. *Id*. at 20 n.52.

[152] *FTC Report on Data Brokers Fails to Address Consumer Privacy Concerns*, EPIC (May 27, 2014), https://epic.org/privacy/choicepoint/ ("The Commission recommended modest legislative changes and failed to address many of consumers' privacy concerns, including profiling and 'scoring' of consumers."); *see also supra* Part II(C)(ii).

[153] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 47.

"help stem the tide of business practices purposefully designed to make a mockery out of the idea of privacy for Americans."[154] The centralized portal, while good in theory, would not satisfy this purpose.

B. Other Legislative Recommendations

In addition to the centralized portal, the FTC recommended that Congress consider legislation requiring data brokers to disclose to consumers on their websites that they not only use raw data collected from sources but also derive data from certain algorithms.[155] Due to the current lack of publicity surrounding data brokers, it is unlikely that most consumers would even visit these websites to learn about this information. Even if a centralized portal existed to increase consumer awareness, merely giving consumers notice of the existence of these derived inferences does not in itself allow consumers access to elements that could qualify as politically sensitive.

Further, the FTC suggested that Congress should require data brokers to disclose the names or categories of their sources of data on their websites so consumers can better correct incorrect data or opt-out of its use.[156] However, due to the convoluted web of data sources, it would be almost impossible for data brokers to disclose a comprehensive list.[157] In order for a consumer to actually correct data, the consumer usually would have to "retrace the path of data through a series of data brokers to finally arrive at the original source."[158] The Commission, in this suggestion to Congress, proposes an abstract solution that is out of touch with reality.

The FTC did not misfire entirely, however—one key recommendation established the *ex ante* controls needed to adequately protect consumers. The FTC Report suggested that Congress require consumer-facing sources—businesses, such as help desks that consumers deal with directly—to obtain consumers' affirmative express consent before collecting and distributing sensitive information.[159] This recommendation, unlike the rest, places the burden of privacy protection on the controller rather than the consumer.[160] Yet the FTC still failed to eliminate industry self-regulation completely. As discussed above, what qualifies as

---

[154] John Eggerton, *Reaction Mixed to FTC Data Broker Report*, B&C (May 27, 2014, 2:57 PM), http://www.broadcastingcable.com/news/washington/reaction-mixed-ftc-data-broker-report/131403 (statement by Jeff Chester, Executive Director of the Center for Digital Democracy).

[155] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 52.

[156] *Id.*

[157] *See id*. at 46.

[158] *Id*. at 14.

[159] *Id*. at 52.

[160] This recommendation would be a necessary step away from the all-too-common privacy self-management model. *See* Solove, *supra* note 86, at 1880 ("Privacy self-management does not provide people with meaningful control over their data.").

"sensitive" is largely discretionary,[161] and consumer protection is not guaranteed. The Commission should have taken it one step further and mirrored the EU Data Directive's requirement that consumer-facing sources obtain affirmative consent for *all* consumer information used in direct marketing,[162] no matter how innocuous. Nonetheless, this suggestion came the closest to hitting the nail on the head in terms of adequate data privacy legislation. The following section addresses why more comprehensive legislation should be established based on specific individual consumer protection provisions within the EU's Data Privacy Directive.

III. THE EUROPEAN WAY OR THE HIGHWAY

The FTC Report as a whole, while aiming for increased transparency in the data broker industry, missed the mark on one crucial point: it placed the burden of mitigating privacy and discrimination concerns on the consumer, rather than on the industry.[163] True amelioration of consumer rights will not be achieved until legislation is enacted which calls both for the increased transparency, and more importantly, accountability, of the data broker industry.[164] Thus, consumer-friendly provisions should be enacted similar to specific individual privacy provisions within the EU's Data Directive, which burden data brokers with privacy management concerns, rather than consumers. First, I will provide relevant background of the EU Privacy Regime that led to the eventual privacy protections of the EU's Data Directive. Then, I will discuss the specific provisions of the Data Directive that should be used to draft a more consumer-friendly legislative framework.

A. The EU's Approach to Data Privacy

Though data privacy laws in the EU are similar to those in the United States with respect to common goals and origins, they differ drastically in their general approach to the protection of personal information.[165] Privacy regulation is triggered when "personally identifiable information" ("PII") is at stake in both regions, but what constitutes PII in the EU and United

---

[161] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 51.

[162] *See* Data Directive, *supra* note 35, art. 14(b).

[163] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, app. C-1 (concurring statement of Commissioner Julie Brill at C-7)*;* Industry regulation is more effective than consumer self-management of privacy. *See* Solove, *supra* note 86, at 1880–81 ("Privacy self-management does not provide people with meaningful control over their data. . . . There are too many entities collecting and using personal data to make it feasible for people to manage their privacy . . . .").

[164] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, app. C-7

[165] Border, *supra* note 45, at 372.

States varies considerably.[166] The Data Directive defines "personal data" broadly as "information relating to an identified or identifiable natural person,"[167] whereas the U.S. definition is far narrower and less consistent.[168] Instead of defining personal information in a coherent manner, privacy law in the United States offers multiple competing definitions.[169] Neither federal nor state law "agree on a single term that identifies the basic category of personal information."[170] The Video Privacy Protection Act (VPPA), for example, defines personally identifiable information as "information that defines a person," whereas the Gramm-Leach-Bliley Act (GLBA) defines personally identifiable information as "nonpublic personal information."[171]

This incongruence largely exists due to the inherent philosophical differences in the two regions.[172] Unlike the United States, the EU views privacy as a fundamental human right.[173] The Convention on Human Rights and Article 8 of the Charter of Fundamental Human Rights recognizes the fundamental right to the protection of personal data.[174] Further, the European Union has recently recognized the "right to be forgotten," which is described as the right to delete "any information related to a data subject."[175] After the Data Directive recognized a general right to Internet protection for individuals, the European Commission took data privacy one-step further by introducing a draft European Data Protection Regulation which specifically included the right to be forgotten.[176] The core provision

---

[166] Schwartz & Solove, *supra* note 54, at 881.

[167] Data Directive, *supra* note 35, art. 2(a).

[168] *See* Schwartz & Solove, *supra* note 54, at 881.

[169] *See* Schwartz & Solove, *supra* note 54, at 887.

[170] *Id.*

[171] This is largely due to the piecemeal approach of the United States regarding data privacy legislation. *Id.* ("When information is identifiable enough to fall within the scope of a particular statute relies . on the specific definition within each privacy statute.")

[172] Schwartz & Solove, *supra* note 54, at 880–81.

[173] Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling,* 98 NW. U. L. REV 63, 90 n.174 (2003) ("Western European governments have long viewed privacy as a fundamental human right.").

[174] Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221, art. 8 §1 (entered into force Sept. 3, 1953), http://www.echr.coe.int/Documents/Convention_ENG.pdf ("Everyone has the right to respect for his private and family life, his home and his correspondence."); Charter of Fundamental Human Rights of the European Union 2000/C, 2000 O.J. (C 364) 1 (EC) art. 8 §1 ("Everyone has the right to personal data concerning him or her.").

[175] Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89 (2012).

[176] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, at 9, COM (2012) 11 final (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (Providing an explanation of Article 17, the "Right to Be Forgotten and to Erasure"); While the "right to be forgotten" is similar to the U.S. system in that it allows consumers to correct or opt-out of publicly available information, it differs from the United States to a considerable extent. Under the "right to be forgotten," a state can require a passive

of the right to be forgotten is simple: "if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from the system."[177] Due to these explicit safeguards, protection of personal data is not a "subject you can bargain about" in the EU.[178]

The Data Directive was first adopted in 1995 and was designed as a comprehensive piece of legislation that aimed to increase the fluidity of cross-border data transfer while simultaneously requiring an absolute recognition of individual privacy rights.[179] The EU's final trade liberalization rules in the Data Directive were strongly influenced by the stringent data privacy protection standards of Germany and France, due to their extensive pull in the market.[180] These political considerations ensured that the Directive's "twin objects"[181] were inseparable, ratcheting up the importance of data privacy in the marketing sphere.[182]

Though "the EU Directive itself does not impose obligations directly on people or businesses," it requires that each EU member state enact laws that govern the processing of personal data in line with its standards.[183] In order to monitor and enforce these laws, each member state must create a data protection authority.[184] To date, all member states have enacted laws in accordance with the Directive's standards,[185] signifying its effectiveness in the EU. Certain consumer-friendly standards embedded in the Directive

---

processor of information like Google to actively interfere with the ability of users to pull up certain kinds of individual information. This does not exist in the United States, where the presumption is against government interference in the free flow of information. *See* Daniel Fisher, *Europe's 'Right to Be Forgotten' Clashes With U.S. Right to Know*, FORBES (May 16, 2014, 8:45 AM), http://www.forbes.com/sites/danielfisher/2014/05/16/europes-right-to-be-forgotten-clashes-with-u-s-right-to-know/ ("The decision [by the Court of Justice of the European Union regarding the "right to be forgotten"] treats search engines like publishers, with the power to pick and choose what other people can see when they type in an individual's name. That conflicts directly with U.S. law, which protects the free flow of information through the First Amendment . . . .").

[177] "[T]he intellectual roots of the right to be forgotten can be found in French law, which recognizes *le droit a l'oubli*—or "the right of oblivion"—a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration." Rosen, *supra* note 175, at 88.

[178] Shaffer, *supra* note 36, at 19.

[179] Border, *supra* note 45, at 372.

[180] Shaffer, *supra* note 36, at 11.

[181] The EU has "twin 'objects,'" which are (1) to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" and (2) to neither restrict nor prohibit the free flow of personal data between Member States." Shaffer, *supra* note 36, at 12.

[182] Shaffer, *supra* note 36, at 11–12.

[183] HARVEY L. KAPLAN, MARK W. COWING, & GABRIEL P. EGLI, SHOOK, HARDY, & BACON L.L.P., A PRIMER FOR DATA-PROTECTION PRINCIPLES IN THE EUROPEAN UNION 37, 40 (2009), http://www.shb.com/attorneys/CowingMark/APrimerforDataProtectionPrinciples.pdf.

[184] Data Directive, *supra* note 35, art. 28.

[185] KAPLAN, COWING, & EGLI, *supra* note 183, at 40.

could work wonders in protecting individuals in the United States, and should be used as a layout for Congress. These particular provisions are explored in depth below.

B. Individual Privacy Protections in the Data Directive: Models for U.S. Legislative Reform

Contrary to the arguments of U.S. officials, "the sum of the parts of U.S. privacy protection is not greater to or equal to the single whole" of Europe's Data Directive.[186] Unlike legislation in the United States, which leaves personal data largely unprotected in the private sector, the Data Directive covers all private sector processing of personal data.[187] Further, the Data Directive levies *ex ante* controls on these data "controllers,"[188] reigning in their ability to "mix, match, buy, sell, and trade profiles and dossiers" containing personal and potentially sensitive consumer information.[189] Upon data collection, the controller must inform the data subject of the controller's identity and the purposes of processing the data.[190] The consumer maintains the right to have inaccurate data corrected, and the right to withhold personal information in some circumstances.[191] Unlike the technical and confusing "opt-out choices" facing consumers in the United States, the Data Directive is clear: consumers have the right to access, correct, and object to the processing of their personal data.[192] Arguably, the most important of these rights is the Directive's explicit right to object, which provides that data subjects can object "at any time on compelling legitimate grounds relating to [their] particular situation to the processing of data relating to [them]."[193] If the objection is successful, the controller may no longer process the piece of data in question.[194] This differs considerably from the U.S. opt-out process in which the opted-out personal information still remains in the data broker's database and can be used later for "anonymous" purposes.[195]

More importantly, the Data Directive contains a provision specific to marketing, requiring that individuals "be informed before personal data [is]

---

[186] Singer, *supra* note 52.

[187] Data Directive, *supra* note 35, art. 2(d).

[188] *Id.*. (The term "controller" is broadly defined to include any "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data").

[189] Shaffer, *supra* note 36 at 26.

[190] Data Directive, *supra* note 35, art.10(c).

[191] *See* Data Directive, *supra* note 35, art.10(c).

[192] Data Directive, *supra* note 35, arts. 12(a), 12(b), 14(a).

[193] *Id.* art. 14(a).

[194] FRA, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 114 (2014), http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

[195] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 43.

disclosed for the first time to third parties for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."[196] Unlike the FTC Report's recommendation requiring affirmative consent for the processing of sensitive information,[197] this provision gives consumers control over *all* information used for direct marketing at the outset. Rather than requiring consumers to find and control their personal data retroactively, EU consumers have *ex ante* control over their data, eliminating the ever-elusive opt-out conundrum[198] facing consumers today. Further, legislation inclusive of this provision would allow consumers to gain control before potentially sensitive or incorrect data is launched into the never-ending black hole of big data exchange.[199]

The third provision that should be used as a roadmap for U.S. legislation is the Data Directive's requirement that Member States prohibit the processing of sensitive information unless an individual affirmatively opts-in to such processing.[200] Unlike in the United States where the term "sensitive" is problematically discretionary,[201] sensitive information covered by the Data Directive includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[202] If a similar provision were adopted in the United States, potentially discriminatory data segments, such as "Bible Lifestyle" or "Leans Left,"[203] would be prohibited from circulation without affirmative consumer consent. This would shield consumers from unequal treatment from direct marketers and would protect them from being placed in offensive or inaccurate data categories, strengthening their position in the market as a whole. As a result, data brokers would no longer be able to freely profile a man as a "Timeless Tradition"[204] on the grounds that he is a retiree who immigrated

---

[196] Data Directive, *supra* note 35, art. 14(b); This differs considerably from the United States, where "retailers also don't make it easy to for you to find out whether they're selling your information." Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 12:59 PM), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

[197] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 52.

[198] *Id*. at 49.

[199] *Id*. at 46 ("[It is] virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers.").

[200] Data Directive, *supra* note 35, art. 8(1).

[201] As discussed above, what counts as "sensitive" varies largely from person to person. Having a fixed standard would decrease the exorbitant amount of self-regulation that exists in American companies today. *See* Ramirez, *supra* note 1, at 51.

[202] Data Directive, *supra* note 35, art. 8(1).

[203] RAMIREZ ET AL., 2014 DATA BROKERS REPORT, *supra* note 1, at 21.

[204] *Id*. at 20 n.52 ("'Timeless Traditions,' which includes 'immigrants, many of retirement age, . . . who have been in the country for 10 or more years,' that 'speak[] some English, but generally prefer[] Spanish and that have 'lower than average' incomes.").

to the United States. Most consumers would refuse to opt-in to such stereotypical categories voluntarily, and consequentially would have much more control over the release and circulation of potentially sensitive information.

These *ex ante* controls alone would help shift the burden of protection from consumers, as suggested by the FTC, to the data brokers compiling, manipulating, and distributing consumer information.[205] The more information consumers are provided with at the outset, the stronger their negotiating positions will be.[206] It should be noted, however, that certain controls are subject to exceptions for business-flexibility purposes, which hinders privacy protections to some extent.[207] Nevertheless, subjecting data brokers to such controls will arguably increase their accountability and transparency in the marketplace.

Further, the EU Directive imposes "*ex post* controls on enterprises," allowing consumers the ability to access, monitor, and challenge personal data post-processing.[208] Adding a similar provision in U.S. legislation would allow American consumers to seek redress for discriminatory or invasive tactics employed by data brokers, while simultaneously increasing the accountability of data brokers.

Last, in contrast with the lack of enforcement running rampant in the U.S. self-regulatory regime,[209] failure to comply with the Directive results in more than just a slap on the wrist. Those who violate the Directive could be subject to two different kinds of liability.[210] First, the Directive requires that each member state establish sanctions for infringement of its provisions.[211] Such sanctions can take the form of fines and/or imprisonment.[212] Germany, for example, has provided for administrative fines of "up to €250,000 per violation—the highest administrative fine in

[205] This is a considerable change from the privacy self-management framework running rampant through the United States, and would ameliorate the bargaining position of individual consumers significantly. *See generally* Solove, *supra* note 86, at 1894.

[206] Shaffer, *supra* note 36, at 34.

[207] Data Directive, *supra* note 35, art.7, (Controllers may process information without consent in instances where the processing is: (i) "necessary for the performance of a contract to which the data subject is party," (ii) "necessary for compliance with a legal obligation," (iii) "necessary in order to protect the vital interests of the data subject," (iv)"necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed," and (v) "necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).").

[208] Shaffer, *supra* note 36, at 26.

[209] Marsh Jr., *supra* note 72, at 555.

[210] KAPLAN, COWING, & EGLI, *supra* note 183, at 40.

[211] Data Directive, *supra* note 35, art. 24.

[212] KAPLAN, COWING, & EGLI, *supra* note 183, at 40.

the EU."[213] Further, in addition to fining violators, French law permits imprisonment for up to five years.[214] In addition to requiring sanctions, the Directive mandates that member states "provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."[215] Thus, there is an explicit provision allowing individuals to recover civilly as well.[216] Adopting similar enforcement tactics in U.S. legislation would give consumers far more redress than provided for in the FTC Report's recommendations to Congress. Rather than waiting for the FTC to flag down companies employing "deceptive business practices,"[217] legislation mirroring this provision would ensure that all data brokers comply with the comprehensive privacy standards outlined above; if they refused, criminal sanctions or civil suits would be waiting.[218] This would not only give consumers control of their personal data, but would also increase the accountability of the predominantly invisible data broker industry.

These specific provisions in the Data Directive should serve as a model for comprehensive legislation in the United States. Congress should stop subordinating privacy and discrimination concerns in favor of the business interests of the marketing sector and make consumer rights a priority. Without adequate comprehensive legislation, consumers will continue to carry the burden of protecting themselves against the privacy infringement and unfair treatment resulting from data brokers' practices.

CONCLUSION

In the words of Anthony Burgess, "To be left alone is the most precious thing one can ask of the modern world."[219] This rings especially true today in a world that is increasingly driven by the vogue for big data.[220] Though the 2014 FTC Report served as an informative privacy wake up call,[221] its bark was much bigger than its bite. The FTC's legislative

---

[213] *Id.* at 46 n.17.
[214] *Id.*
[215] Data Directive, *supra* note 35, art. 23(1).
[216] KAPLAN, COWING, & EGLI, *supra* note 183, at 40.
[217] *See* Marsh Jr., *supra* note 72, at 555.
[218] It should be noted that only the Department of Justice (DOJ) has the power to seek criminal sanctions. The FTC, however, may refer matters to the DOJ for criminal enforcement. *See, e.g.*, 15 U.S.C. § 46(k) (2006).
[219] ANTHONY BURGESS, HOMAGE TO QWERT YUIOP: ESSAYS (1986).
[220] Kakaes, *supra* note 19.
[221] Lohr, *supra* note 24 (statement by Jeffrey Chester, Executive Director of the Center for Digital Democracy).

recommendations lacked the teeth necessary to address the current privacy and discrimination concerns facing American consumers today. The practices of data brokers, in particular the aggregation of raw data into potentially discriminatory categories, do more than just impose upon a consumer's "right to be let alone."[222] They also subject individuals to unfair and predatory practices, differential pricing, and other negative treatment by marketing companies.[223]

This Comment serves as a call for Congress to stop sporadically reacting to data privacy concerns. Instead, it must proactively pass comprehensive legislation mirroring the Data Directive's individual protections. Regulations must be imposed *ex ante*, rather than *ex post*, and the only way to do this is to abandon the self-regulatory approach of data brokers completely. It is time for Congress to act. The question remains if it will.

[222] Warren & Brandeis, *supra* note 38, at 213 n.1.
[223] S. COMM. ON COMMERCE, SCI., & TRANSP., *supra* note 10, at 6.