The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era

Brittany A. Martin[*]

ABSTRACT: In the United States, there is a billion-dollar industry that revolves around consumer data, but most consumers do not know it exists. Data brokers are companies that collect information from consumers to buy and sell. These companies also derive further valuable information from consumers. Data brokers use their data for several things, one of which is for marketing purposes. In the United States, there is no legislation on the federal level to regulate the collection and use of this data by data brokers. The United States has failed its consumers by not providing regulation. There are a few states that have taken initiative to protect consumer data online, namely Vermont and California. Additionally, the European Union recently implemented the General Data Protection Regulation ("GDPR"). The GDPR provides a vast range of protection for EU citizens concerning their online data. Congress should follow guidance from Europe, California, and Vermont regarding digital consumer privacy. Congress should include in its legislation: a meaningful notice-and-choice requirement, an option for consumers to have access to and the ability to edit data held by data brokers, require companies to minimize the amount of the data that they collect and retain, have strict penalties for noncompliance, and create quasi-governmental entities to assist in regulation.

[*] J.D. Candidate, The University of Iowa College of Law, 2020; B.A., The University of Iowa, 2017.

I. INTRODUCTION

If you are a consumer in the United States who uses the Web, the chances are high that you see a plethora of advertisements while you browse. This is often true regardless of whether you are actively online shopping. Perhaps you have been online shopping, moved on to something else, and then see an item you previously lingered on but did not buy. With the average American spending 23.6 hours a week online,[1] this is a common experience for many.[2] While these targeted ads can sometimes be helpful, other times they serve as an unwanted temptation or simply an annoyance. Some individuals may also find them creepy.

1. HARLAN LEBO, THE 2017 DIGITAL FUTURE REPORT: SURVEYING THE DIGITAL FUTURE 6 (2017), *available at* http://www.digitalcenter.org/wp-content/uploads/2013/10/2017-Digital-Future-Report.pdf [https://perma.cc/ZRE7-UD5H].

2. Christopher Elliot, *Why Does That Online Ad Keep Following Me?*, USA TODAY (Nov. 6, 2016, 6:01 PM), https://www.usatoday.com/story/travel/advice/2016/11/06/retargeting-online-ads/93282408 [https://perma.cc/9JTK-MSBM].

The idea gets creepier once you explore the reason behind these ads popping up on your computer or mobile device. On every site you visit on the Web, there are often several entities following you around as you browse.[3] These entities study you extensively; they learn demographics such as age, location, and interests.[4] Once these entities have a sufficient level of information, they are able to target you more accurately.[5] Some of these entities are commonly known and used by consumers, such as Facebook or Twitter; however, there are several other companies you have probably never heard about that exist solely to collect consumer information. These include Acxiom, Experian, Datalogix, and Statlistics.[6] At least some of these companies likely have information about you in their databases right now.[7] If you are unaware of the data broker industry, you are not alone; it keeps a low profile.[8] There would also be no reason for you to know who they are, since you have likely never interacted with one directly.

One may wonder why these companies have so much information about you when you know so little about them. The answer to that question is that there is no federal regulation of the collection of consumer data for marketing purposes.[9] Data brokers and companies you interact with are free to collect and sell your data without your knowledge. One may have a problem with this for several reasons. For starters, it seems to be an invasion of consumer privacy. After all, in "real life," a regular person would not let a stranger follow them around the mall taking notes on their behavior and to report them back to some company they have never heard of—which begs the question: Why is this practice okay when it is done online?

Another concern is related to the security practices of big data companies. In 2018, there was a swarm of data breaches, affecting millions all around the world.[10] The European Union ("EU") has taken the threat to online privacy seriously by enacting the General Data Protection Regulation

3. Max Eddy, *How Companies Turn Your Data into Money*, PCMAG (Oct. 10, 2018, 8:00 AM), https://www.pcmag.com/article/364152/how-companies-turn-your-data-into-money [https://perma.cc/Y8SN-TS53].

4. *Id.*

5. *Id.*

6. Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016, 2:30 PM), https://www.newsweek.com/secretive-world-selling-data-about-you-464789 [https://perma.cc/7RPT-8ZCF].

7. *Id.*

8. *Id.*

9. *Id.*; Eddy, *supra* note 3.

10. Kyunghee Park & Jinshan Hong, *Millions of Passengers Hit in Worst Ever Airline Data Hack*, BLOOMBERG (Oct. 24, 2018, 7:02 PM), https://www.bloomberg.com/news/articles/2018-10-25/cathay-pacific-reports-data-breach-affecting-9-4-million-fliers [https://perma.cc/7J9N-NSF5]; Jacob Taylor, *Ticketmaster Data Theft Part of Larger Credit Card Scheme, Security Firm Says*, NBC NEWS (July 10, 2018, 12:33 PM), https://www.nbcnews.com/business/business-news/ticketmaster-data-theft-part-larger-credit-card-scheme-security-firm-n890206 [https://perma.cc/9YLP-L4V8].

("GDPR").[11] The GDPR provides expansive protection for the online privacy of European Citizens and data collected and processed within the EU.[12] In the United States, legislation at the federal level is scant and under-protective.[13]

Some states, such as California and Vermont, have passed their own laws to protect consumers.[14] The question remains as to whether the United States, at the federal level, will follow suit regarding the protection of its consumers' online privacy.

This Note argues that the United States should take initiative to protect consumer data by passing legislation on the federal level. Part II of this Note delves into what exactly a data broker is and will explore the background of data privacy laws both in the United States and Europe. In Part III, this Note explains why there is a need for change on the federal level. This Note takes a critical stance on the lack of transparency of the data broker industry. It also details the lack of consumer trust regarding big data companies, given the frequency with which data breaches occur. There are also concerns about discrimination stemming from data collection. Part IV of this Note will propose specific solutions that Congress should adopt in federal legislation in order to protect consumer privacy online.

II. WHO DATA BROKERS ARE AND HOW THEY ARE REGULATED

Part II of this Note will provide a comprehensive overview of the data broker industry, ranging from exactly what a data broker is, to how these entities operate, and finally to how they are currently regulated. Section II.A will define what data brokers are and explain what they do with consumer data. Section II.B will analyze current regulation of data brokers on the federal level: looking at legislation, administrative protections, and judicial protection of consumer privacy. Section II.C will explore consumer protection of online privacy at the state level, with both California and Vermont serving as leaders. Once regulation in the United States has been explored, Section II.D of this Note will move across the pond to Europe and detail important provisions of the GDPR that provide a vast array of protection of online protection to European citizens.

A. DATA BROKERS AND HOW THEY COLLECT AND USE CONSUMER DATA

The data broker industry is largely unknown to consumers, so it is helpful to explore exactly who these companies are and what they do. In order to

11. Warwick Ashford, *GDPR Driving Data Protection Maturity*, COMPUTER WKLY. (Oct. 31, 2018, 12:00 PM), https://www.computerweekly.com/news/252451669/GDPR-driving-data-protection-maturity [https://perma.cc/NM9B-7GL7].

12. *Id.*

13. *See infra* Section II.B.1.

14. *See infra* Section II.C.

understand why regulation is necessary, one must understand exactly what a data broker is. Finally, knowing what data brokers are and how they gather data, and knowing how they use that information clarifies the need for regulation.

The definition of a "data broker" is widely debated. For the purpose of this Note, "[d]ata brokers are companies that collect personal and non-personal information about individuals and license, sell, share or allow use of that information by another entity for the other entity's benefit or for their mutual benefit."[15] There are several different types of data brokers; some interact with consumers and others do not.[16] This Note will focus on third-party data brokers—companies that have no relationship with the consumer.[17] Unfortunately, since these companies do not interact with consumers, most consumers do not know they exist.[18]

Data brokers are no new concept; they have existed for many years. In the 1960s, data brokers collected much of their information offline.[19] One type of information data brokers collected is known as personally identifiable information ("PII"), defined as "information that can be used to distinguish or trace an individual's identity."[20] As technology and the Internet advanced, data brokers began collecting information online, anonymously, via cookies; this information is considered non-personally identifiable information ("Non-PII").[21] Today, data brokers collect both types of information in order to further their interests. The following Sections will explore how data brokers currently obtain the information that they do and what they do with that information.

There are several different types of third-party data brokers. These include people-search websites, Consumer Reporting Agencies ("CRAs"), risk mitigation services, and marketing data brokers.[22] Each of these categories of data brokers are regulated differently, as will be discussed later in this Note.[23] Among the categories, marketing data brokers are of particular concern. One

15. Jennifer Barrett Glasgow, *Data Brokers: Should They Be Reviled or Revered?*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 25, 26 (Evan Selinger et al. eds., 2018).

16. *Id.*

17. *Id.*

18. *See* EDITH RAMIREZ ET AL., FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 3 (2014).

19. Glasgow, *supra* note 15.

20. *Rules and Policies—Protecting PII—Privacy Act*, U.S. GEN. SERVS. ADMIN., https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act [https://perma.cc/6J2C-NZ86]; *see also* Glasgow, *supra* note 15 ("Historically, data brokers . . . in the 1960s dealt primarily with personally identifiable information (PII), such as names, addresses, and telephone numbers." (footnote omitted)).

21. Glasgow, *supra* note 15.

22. *Id.*

23. *See infra* Section II.B.1.

thing remains true across each category—the lack of transparency in the data broker industry is problematic.[24]

1. How Do They Know That?

One may wonder how data brokers gather the information that they have. In 2014, the Federal Trade Commission ("FTC") wanted to answer that very question, so it conducted an investigation.[25] In order to conduct a thorough examination of data brokers, the FTC ordered nine different data brokers from various categories to provide information "about each data broker's products and services, data collection practices, the sources of its data, its clients, and the extent to which it provides consumers with access to and control of their information."[26]

The FTC found that data brokers get their information from a variety of places. One source of information on consumers was the federal government,[27] including public records such as the U.S. Census Bureau.[28] The census provides a vast amount of information, including geographic location cross-referenced with "ethnicity, age, education level, household makeup, income, occupations, and commute times."[29] Information gathered by data brokers also came from state and local governments, including professional licenses, recreational licenses, and real property information.[30] Additionally, data brokers collected information from other publicly available sources such as blogs and social media pages where individuals had limited protection settings.[31]

Data brokers also collect data from commercial sources, such as retailers.[32] This "information can include the types of purchases . . . , the dollar amount of the purchase, the date of the purchase, and the type of payment used."[33] Some of the data brokers received this information directly from the retailer, while others purchased the information from other data brokers.[34] Such sharing creates a large web of data exchanges, which makes it

---

24. RAMIREZ ET AL., *supra* note 18, at 4.

25. *See generally id.* (providing a thorough analysis of data brokers, including how they collect information and how they use it; the FTC also provided suggestions for regulations and best practices moving forward).

26. *Id.* at 7. The companies the FTC investigated were: Acxiom, a marketing data broker; Corelogic, a CRA; Datalogix, a marketing broker; eBureau, a marketing broker; ID Analytics, a people-search broker; Intelius, a CRA; PeekYou, a marketing broker; Rapleaf, a people-search broker; and Recorded Future, a marketing broker. *Id.* at 8–9.

27. *Id.* at 11.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.* at 13.

32. *Id.*

33. *Id.*

34. *Id.* at 14.

"virtually impossible for a consumer to determine the originator of a particular data element."[35]

Data brokers collect our online information by using cookies. Cookies were originally designed to allow websites to remember who web-page visitors are.[36] Once companies realized they could use this technology to track consumer movement, "the third-party cookie was born."[37] Now consumers are tracked, typically by multiple entities, each time they surf the web—not only when they use their computers,[38] but also when using smartphone browsers or various apps.[39]

Although cookies are "inherently anonymous," categorizing them as non-PII, individuals often voluntarily identify themselves.[40] Therefore, data brokers have an extensive amount of personal information about a staggering number of consumers, largely without consumer knowledge. One of the companies the FTC studied, Acxiom, boasted that "[i]ts databases contain information about 700 million consumers worldwide with over 3000 data segments for nearly every U.S. consumer."[41] In some instances, data brokers may know more about individuals than even their friends or family.[42]

Although data brokers are collecting vast amounts of information, the FTC had serious concerns about the accuracy of that data.[43] According to one study by Deloitte, more than two-thirds of individuals they surveyed indicated brokered information about them was "0 to 50% [accurate] as a whole."[44] Additionally, very few brokers that participated in the FTC study provided consumers with the opportunity to edit their data.[45] This was also true of the

35. *Id.*

36. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 47–48 (2015).

37. *Id.* at 48.

38. *Id.* ("One reporter discovered that 105 different companies tracked his Internet use during one 36-hour period.").

39. *Id.*

40. *Id.* at 49.

41. RAMIREZ ET AL., *supra* note 18, at 8.

42. For example, Target created pregnancy scores to predict when certain consumers were pregnant. Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did [https://perma.cc/U687-9PGA]. Although Target is a consumer-facing company, it used tactics similar to those that would be employed by third-party data brokers. *Id.* In the Target case, a teenage girl's father found out about her pregnancy via these targeted ads. *Id.*

43. RAMIREZ ET AL., *supra* note 18, at 53–54.

44. John Lucker et al., *Predictably Inaccurate: The Prevalence and Perils of Bad Big Data*, DELOITTE INSIGHTS (July 31, 2017), https://www2.deloitte.com/insights/us/en/deloitte-review/issue-21/analytics-bad-data-quality.html [https://perma.cc/RX2F-Z5UG]. This study provides several useful specifics in understanding the prevalence of inaccurate data collected and stored by data brokers.

45. RAMIREZ ET AL., *supra* note 18, at 49.

Deloitte study.[46] Therefore, while brokers may have a great deal of information, this information is often inaccurate.

2. What Do Data Brokers Do with This Data?

One may wonder what data brokers are doing with all the information they have. The answer is multifaceted. Data brokers sell some of the data, and they also use the raw data to derive additional data about consumers.[47] Data brokers use information about consumer purchases "to predict an interest, analyze the characteristics the consumers share, and use the shared characteristic data to create a predictive model to apply to other consumers."[48] The categorized consumers are placed in "data segments."[49] These data segments are used for targeted marketing.[50] For example, if an individual purchases baking supplies, they may be placed in a data segment called "Interested in Baking" and receive coupons for baking supplies. Such a segment is seemingly harmless, but others are more troubling—like segments that "focus purely on consumers' financial status, such as 'Underbanked Indicator,' 'Credit Worthiness,' 'Invitation to Apply Offers —Bankcard Utilization Rate,'" and several others.[51] These kinds of data segments run the risk of discrimination against certain consumers.[52] Other segments contain private information, such as whether a consumer has HIV or diabetes.[53]

B. FEDERAL REGULATION OF DATA BROKERS IN THE UNITED STATES

Currently, there are some protections for consumers of their online information in the United States. Section II.B will explore federal protection of consumer privacy online in the United States. In Section II.B.1, this Note will look at how Congress protects digital privacy. Section II.B.2 will explore consumer protection of digital privacy at the administrative level. Finally, Section II.B.3 details protection of consumer privacy at the judicial level.

1. Congressional Protection of Digital Consumer Privacy

There is no sweeping federal legislation regulating the data broker industry; instead, there are a variety of laws that protect different types of

46. Lucker et al., *supra* note 44.

47. RAMIREZ ET AL., *supra* note 18, at 19.

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.* at 20. For a more extensive list of data segments, see *id.* at B-3 to B-6 (listing numerous data segments ranging from "Affluent Baby Boomer" to "Winter Activity Enthusiast").

52. SCHNEIER, *supra* note 36, at 109.

53. RAMIREZ ET AL., *supra* note 18, at 51.

information.[54] The Fair Credit Reporting Act ("FCRA") provides protection of consumer credit information.[55] The Health Insurance Portability and Accountability Act ("HIPAA") protects medical information.[56] The Gramm–Leach–Bliley Act ("GLBA") regulates financial institutions to protect the personal finance information of consumers.[57] The Children's Online Privacy Protection Act ("COPPA") protects children's privacy online.[58] Additionally, due to advancements in technology, some data remains unprotected.[59] None of these federal regulations cover the use of consumer data for marketing purposes.[60]

There have been some recent attempts at the Congressional level to increase protection of consumers' digital privacy. On April 10, 2018, Senator Edward Markey of Massachusetts proposed the Customer Online Notification for Stopping Edge-provider Network Transgressions Act ("CONSENT Act").[61] The CONSENT Act would provide a broad range of protection for consumers online. Although the CONSENT Act does not mention data brokers specifically, several of its provisions would affect the data broker industry. For instance, the CONSENT Act would require the FTC to issue regulations that require consumer-facing entities to disclose "the types of entities with which the edge provider shares sensitive customer proprietary information."[62] The CONSENT Act would also require edge providers (internet service websites) to "obtain opt-in consent from a customer to use, share, or sell the sensitive customer proprietary information of the customer."[63] Overall, the CONSENT

54. Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 787 (2016).

55. Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2012).

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

57. Gramm–Leach–Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

58. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012). For a breakdown of the various laws protecting certain types of data, see Glasgow, *supra* note 15, at 39–44.

59. Lipman, *supra* note 54, at 788 (providing the example that medical information collected from a FitBit or similar technology is not protected under HIPAA).

60. RAMIREZ ET AL., *supra* note 18, at i.

61. Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S. 2639, 115th Cong. § 2 (2018). An identical bill was also proposed in the House of Representatives by Representative Michael Capuano of Massachusetts on May 15, 2018. Customer Online Notification for Stopping Edge-provider Network Transgressions Act, H.R. 5815, 115th Cong. § 2 (2018).

62. S. 2639, § 2(b)(2)(B)(i)(III).

63. *Id.* § 2(b)(2)(B)(iii); *see also* Margaret Rouse, *Definition: Edge Provider*, TECHTARGET, https://whatis.techtarget.com/definition/edge-provider [https://perma.cc/SPX7-H7DV] ("[A]n edge provider is a website, web service, web application, online content hosting or online content delivery service that customers connect to over the internet. Edge providers, which include Google, Amazon, Netflix and Facebook, use the customer's internet service provider (ISP) to deliver content.").

Act encourages transparency and accountability in entities that collect consumer information online.

There has also been proposed legislation specifically targeting data brokers. The "Data Broker Accountability and Transparency Act of 2018" was proposed by House Representative Henry Johnson of Georgia on July 26, 2018.[64] This Act would provide the FTC with enforcement power.[65] Under this law, data brokers would be required to provide access to personal information held by the entities.[66] Additionally, consumers would have the opportunity to edit inaccurate information available to them.[67] Furthermore, consumers could choose to opt out of the collection of their data for marketing purposes.[68] The Act allows for a civil penalty not greater than $16,000.[69] Several similar bills have been proposed in both the House and the Senate, but have failed to pass.[70] It seems unlikely that the 2018 version of the bill would receive any different treatment.

Although Congress has not passed any legislation, it has shown growing interest in consumer privacy online. On September 26, 2018, the Senate Commerce Committee held a hearing regarding consumer privacy.[71] Several big-name technology companies, including Amazon, Apple, AT&T, Charter, Google, and Twitter attended the hearing.[72] Noticeably absent, however, were any representatives from the data broker industry.[73] This could be an

64. Data Broker Accountability and Transparency Act of 2018, H.R. 6548, 115th Cong.

65. *Id.* § 7(a)(2)(A).

66. *Id.* § 5(b)(1).

67. *Id.* § 5(c).

68. *Id.* § 5(e)(2).

69. *Id.* § 7(b)(2)(A).

70. Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong.; Data Broker Accountability and Transparency Act of 2016, H.R. 4516, 114th Cong.; Data Broker Accountability and Transparency Act of 2015, S. 668, 114th Cong.; Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014).

71. Dan Tynan, *Silicon Valley Finally Pushes for Data Privacy Laws at Senate Hearing*, GUARDIAN (Sept. 26, 2018, 7:33 PM), https://www.theguardian.com/technology/2018/sep/26/silicon-valley-senate-commerce-committee-data-privacy-regulation [https://perma.cc/VR99-2D6N].

72. *Id.* In opening statements, majority leader Chairman John Thune said:

> I believe, there is a strong desire by both Republicans and Democrats, and by both industry and public interest groups, to work in good faith to reach a consensus on a national consumer data privacy law that will help consumers, promote innovation, reward organizations with little to hide, and force shady practitioners to clean up their act.

Examining Safeguards for Consumer Data Privacy Before the S. Comm. on Commerce, Sci., & Transp., 115th Cong. (2018) (statement of Sen. John Thune, Chairman, S. Comm. on Commerce, Sci., & Transp.), *available at* https://www.commerce.senate.gov/public/index.cfm/hearings?Id=2FF829A8-2172-44B8-BAF8-5E2062418F31&Statement_id=E18C1B83-51D1-4C57-BCC8-047DCBAAA26D [https://perma.cc/T36L-CA9R].

73. Joseph Jerome, *Where Are the Data Brokers?*, SLATE (Sept. 25, 2018, 7:30 AM), https://slate.com/technology/2018/09/data-brokers-senate-hearing-privacy.html [https://perma.cc/M3S2-VLN3] ("The reality is that while many companies now collect a whole lot of our

indication that data brokers prefer to remain largely unknown to consumers while the big-name companies sort out legislation at the federal level. Congress has not only heard from big technology companies, though; on October 10, 2018, the Senate Commerce Committee also heard from consumer advocacy groups about online privacy.[74] These hearings could be a step in the right direction towards passing legislation at the federal level regarding consumer privacy and data security. Whether this would be through one of the already-proposed bills or a new bill is unclear; it remains to be seen whether Congress will enact anything at all.

2. Protection of Digital Consumer Privacy at the Administrative Level

Although Congress has not provided much protection of digital consumer privacy, a different avenue for protection may be the FTC. Without congressional authority to regulate data brokers, the FTC's powers are limited; yet, one provision that provides the FTC with some authority is section 5 of the Federal Trade Commission Act.[75] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[76] This provision provides the FTC with some leeway when seeking out "blatantly" deceptive companies.[77]

The FTC used its section 5 authority to regulate Snapchat, a social media app.[78] Snapchat led its users to believe that their messages were instantly deleted when there was really a simple workaround for individuals to save

information, there's really only one industry that doesn't want us to know much about it in exchange. Data brokers may know everything about you—but they still don't want you to know about them.").

74. India McKinney & Gennie Gebhart, *New Witness Panel Tells Congress How to Protect Consumer Data Privacy*, ELECTRONIC FRONTIER FOUND. (Oct. 11, 2018), https://www.eff.org/deeplinks/2018/10/new-witness-panel-tells-congress-how-protect-consumer-data-privacy [https://perma.cc/CF4C-5TYW]. In Chairman Thune's opening statement for this hearing, he said:

> I want to be clear that the next federal privacy law will not be written by industry. Any federal privacy law should incorporate views from affected industry stakeholders and consumer advocates in an effort to promote privacy without stifling innovation. With that in mind, today's hearing will focus on the perspectives of privacy advocates and other experts. We will also continue to solicit input from additional stakeholders in the days ahead.

Press Release, John Thune: U.S. Senator for S.D., Thune Leads Second Hearing Examining Safeguards for Consumer Data Privacy (Oct. 10, 2018), *available at* https://www.thune.senate.gov/public/index.cfm/2018/10/thune-leads-second-hearing-examining-safeguards-for-consumer-data-privacy [https://perma.cc/3JAD-YX2Q].

75. Federal Trade Commission Act, Pub. L. No. 63-203, ch. 311, § 5, 38 Stat. 717, 719–21 (1914) (codified as amended at 15 U.S.C. § 45 (2012)).

76. 15 U.S.C. § 45(a)(1).

77. Lipman, *supra* note 54, at 789–90.

78. Press Release, FTC, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were [https://perma.cc/4HME-EAJQ].

them.[79] According to the FTC, Snapchat also "misrepresented its data collection practices."[80] These revelations led Snapchat to consent to "implement[ing] a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years."[81] The FTC has used its section 5 authority to obtain consent agreements with other large technology-based companies as well, including some data brokers.[82] Snapchat and other companies have agreed to be monitored; however, section 5 does allow the FTC to enforce its power through administrative adjudication.[83] Section 5 has proved a useful tool for the FTC, but the agency can only employ it when companies have actually misled their consumers.[84] As a result, a company could "be vague about its commitment to privacy" to avoid a section 5 violation.[85] The FTC has successfully used its section 5 power to address data security in the breach context.[86] The FTC's power has been challenged by some, but for the moment it seems that the FTC will be permitted to continue using it.[87] The FTC does what it can to protect consumers online, but its power is limited.

---

79. *Id.*

80. *Id.*

81. *Id.*

82. *See* Glasgow, *supra* note 15, at 42 (explaining that ChoicePoint and Spokeo, both data brokers, have entered into consent agreements with the FTC). As the FTC explained:

> Spokeo, Inc., a data broker that compiles and sells detailed information profiles on millions of consumers, will pay $800,000 to settle Federal Trade Commission charges that it marketed the profiles to companies in the human resources, background screening, and recruiting industries without taking steps to protect consumers required under the Fair Credit Reporting Act.

Press Release, FTC, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 12, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed [https://perma.cc/G2SU-QHJZ]. The ChoicePoint deal had the following requirements:

> The order requires ChoicePoint to establish, implement, and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from or about consumers. It also requires ChoicePoint to obtain, every two years for the next 20 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order.

Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million [https://perma.cc/2JBB-E5BC].

83. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/J5TB-A9CE].

84. *See* Lipman, *supra* note 54, at 790.

85. *Id.*

86. *See id.* at 790–91.

87. *Id.*

Another administrative agency, the National Telecommunications and Information Administration ("NTIA"), has recently shown interest in protecting consumers' digital privacy.[88] On September 21, 2018, the NTIA issued a request for public "comment[] on ways to advance consumer privacy while protecting prosperity and innovation."[89] The NTIA set forth two specific goals moving forward: "(1) A set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and (2) a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections."[90] The NTIA had a great response, and published over 150 comments.[91] Large tech companies such as Google, Amazon, and Microsoft contributed comments, as did consumer advocates such as the Center for Digital Democracy, Californians for Consumer Privacy, and the Electronic Privacy Information Center.[92]

Google stated that it "firmly believes that federal legislation is the best path to realize NTIA's stated goals, and reaffirms our long-standing support for smart and strong comprehensive baseline privacy legislation that enshrines high standards of privacy for everyone."[93] Google further emphasized the importance of "Individual-Centric Privacy Outcomes" regarding transparency, control of data processing, responsible collection of data, and security.[94] Both Amazon and Microsoft echoed these sentiments.[95] Large tech companies appear to be supportive of the NTIA's goals. On the consumer protection side, the Center for Digital Democracy criticized the NTIA's goals as too broad, and encouraged the agency to elaborate on its

88. Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,600 (Sept. 21, 2018).

89. *Id.*

90. *Id.* at 48,601.

91. *Comments on Developing the Administration's Approach to Consumer Privacy*, NAT'L TELECOMM. & INFO. ADMIN. (Nov. 13, 2018), https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy [https://perma.cc/46ZC-S7FM].

92. *Id.*

93. Comment Letter from Google to Nat'l Telecomms. & Info. Admin. on Developing the Administration's Approach to Consumer Privacy 2, *available at* https://www.ntia.doc.gov/files/ntia/publications/google_comments_for_ntia_rfc_on_privacy.pdf [https://perma.cc/GGU3-KWDR].

94. *Id.* at 3–6.

95. *See* Comment Letter from Brian Huseman, Vice President of Public Policy, Amazon, to David J. Redl, Assistant Sec'y, Nat'l Telecomms. & Info. Admin. on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/amazon_ntia_privacy_comment_11-9-2018.pdf [https://perma.cc/X5PJ-G96A]; Comment Letter from Microsoft to Nat'l Telecomms. & Info. Admin. on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/msft_response_to_ntia_privacy_rfc.pdf [https://perma.cc/R3CQ-PV7H].

outcomes.[96] The Electronic Privacy Information Center ("EPIC") echoed these sentiments, along with suggesting the creation of a new agency for data protection.[97] Furthermore, EPIC discouraged harmonizing the regulatory landscape and instead suggested creating a federal baseline, which would allow states to supplement with their own more-protective privacy laws.[98]

Across the politically accountable branches of the federal government, there seems to be a push toward some sort of regulation to protect consumers' digital privacy. Additionally, private companies have expressed interest toward comprehensive legislation to both Congress and administrative agencies. Consumer interest groups also support federal data privacy legislation. For the time being, regulation of data brokers at the federal level is unpredictable and often under-protective; for some types of information, it is nonexistent.

3. Judicial Treatment of Invasions of Digital Privacy

Courts rarely adjudicate matters involving data brokers, but there are some cases that speak to data security more generally. The most notable case involving a data broker was *Spokeo, Inc. v. Robins*.[99] Spokeo is a people-search data broker.[100] The issue in the *Spokeo* case was that the company had inaccurate information about an individual, Robins, who sued them under the Fair Credit Reporting Act ("FCRA").[101] The Supreme Court did not decide on the merits of the case, but rather addressed the issue of standing.[102] On remand, the Ninth Circuit held that Robins established a concrete injury under the FCRA because Spokeo *published* inaccurate information about him.[103]

Although judicial relief is readily available for individuals like Robins whose stolen information falls into a protected category such as credit card information,[104] plaintiffs may have more difficulty if their information is

96. Comment Letter from Katharina Kopp, Deputy Dir., Ctr. for Dig. Democracy, to David J. Redl, Assistant Sec'y, Nat'l Telecomms. & Info. Admin. on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/cddcomments18082178o-8780-01.pdf [https://perma.cc/3E5N-ZWNK].

97. Comment Letter from Marc Rotenberg, President, Elec. Privacy Info. Ctr., and Christine Bannan, Consumer Prot. Counsel, Elec. Privacy Info. Ctr., to Nat'l Telecomms. & Info. Admin. on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/epic-ntia-nov2018.pdf [https://perma.cc/8NPD-QEU6].

98. *Id.*

99. Spokeo, Inc. v. Robins (*Spokeo II*), 136 S. Ct. 1540, 1546 (2016).

100. *Id.*

101. *Id.* at 1544; *see also supra* Section II.A.1.

102. *Spokeo II*, 136 S. Ct. at 1547. The Court ultimately remanded the case back to the Ninth Circuit because in order to make a proper distinction about whether an injury is both "concrete[] and particulariz[ed]." *Id.* at 1550.

103. Robins v. Spokeo, Inc., 867 F.3d 1108, 1116 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 931 (2018).

104. *See supra* Section II.B.1.

merely compromised or does not fall into a protected category. When someone's private information has been compromised but the plaintiff cannot prove that a third party actually used sensitive information, it is difficult to achieve standing.[105] It is possible for plaintiffs to achieve standing if they are able to show their information was merely compromised but not utilized.[106] This was true when dealing with consumers' credit information,[107] especially because such information is much more sensitive than name, address, phone number, etc.[108] It is difficult to see how lack of protection for such seemingly harmless information would be treated the same as compromised credit card information. For this reason, consumers can expect little redress in court if data brokers compromise mere identifying information (such as name, phone number, and address), unless they can prove such a compromise led to or there is a "substantial risk" of a serious injury like identity theft or fraud.[109]

Not all hope is lost regarding protection of consumer privacy by the judiciary. In *FTC v. Vizio, Inc.*, the New Jersey Attorney General and the FTC brought a complaint against Vizio, a television company.[110] Vizio was using Internet-connected televisions to "continuously track what consumers are watching, and transmit[ting] that information to [Vizio]."[111] According to the complaint, Vizio did this "on a second-by-second basis."[112] Additionally, Vizio "provided consumers' data to third parties for the purpose of targeting advertising to particular consumers on their other digital devices based on their television viewing data."[113] Plaintiffs alleged that Vizio did not provide adequate notice to consumers about these practices, and that this was unfair as defined by law.[114] The parties ultimately settled the case, resulting in a stipulated order requiring Vizio to provide notice to its consumers of their practices and to obtain consent from them.[115] The order focused on Vizio's

105. *See generally* Hinton v. Heartland Payment Sys., Inc., No. 09-594 (MLC), 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (holding that where plaintiff could not prove his credit information had been used at his expense, there was no injury in fact).

106. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016) (overruling the lower court's holding that the plaintiffs lacked standing because there was a "substantial risk" that harm might occur).

107. *Id.* at 388.

108. *Id.* ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.").

109. *Id.*

110. Complaint for Permanent Injunction and Other Equitable and Monetary Relief at 1, FTC v. Vizio, Inc., No. 2:17-CV-00758-SRC-CLW, 2017 WL 7000553 (D.N.J. Feb. 14, 2017).

111. *Id.* at 4.

112. *Id.*

113. *Id.* at 5.

114. *Id.* at 7–8.

115. Stipulated Order for Permanent Injunction and Monetary Judgment at *3–5, FTC v. Vizio, Inc., No. 2:17-CV-00758-SRC-CLW, 2017 WL 7000553 (D.N.J. Feb. 14, 2017). The Order

actions, a consumer facing entity, but the order ultimately will affect third-party data brokers given the requirement that consumers must consent to the collection of their information. This case suggests that there is some protection of online consumer privacy happening at the judicial level.

There is currently a case in the Middle District of Florida regarding the Exactis breach.[116] A Florida resident, Kenneth Heretick, brought a class action suit claiming that the "case concerns one of the biggest and most damaging data breach cases, exceeding Equifax and other massive data breaches—in both scale and information disseminated."[117] Heretick is alleging Exactis' "negligence, negligence per se, and unjust enrichment," along with violation of state consumer protection laws for a sub-class of plaintiffs.[118] The plaintiffs are alleging that they have been harmed by Exactis' negligence in exposing personal information such as "phone numbers, home and email addresses, personal interests and preferences, ages and genders of their children, and other extremely detailed, personal information—exceeding as many as 400 data points on each business and consumer."[119] The plaintiffs further allege that they have been injured by the looming potential of fraud and the surveillance of their credit information that is necessary because of that concern.[120] It remains to be seen whether the case will go to trial, and if it does, whether anything will come of it—but it seems unlikely that these plaintiffs will succeed since they cannot yet prove their information has been used for fraudulent purposes.

C. STATE REGULATION OF DATA BROKERS

Both California and Vermont have proven to be leaders in protecting consumer privacy online. Section II.C.1 will explore the California Consumer Protection Act of 2018 ("CCPA"). Through the CCPA, California will implement the most expansive protection of consumers' online privacy in the United States. Additionally, Vermont recently passed legislation aimed at regulating data brokers specifically, which is an important recognition of the need to regulate this industry. Section II.C.2 will discuss the Vermont law.

1. The California Consumer Privacy Act of 2018

Several states in the United States have taken it upon themselves to protect consumer privacy by regulating data brokers.[121] California has been a

requires notice to be "[p]rominently disclose[d]" and "separate and apart from any 'privacy policy,' 'terms of use' page, or other similar document." *Id.* at *2.

116. Class Action Complaint Jury Trial Demanded, Heretick v. Exactis, LLC, No. 3:18-cv-00822-BJD-PDB (M.D. Fla. June 28, 2018).

117. *Id.* at 1.

118. *Id.* at 5.

119. *Id.* at 1.

120. *Id.* at 10–12.

121. For a brief overview of various state regulation, see Glasgow, *supra* note 15, at 42.

strong leader in online privacy laws. The State has a rich history of passing several laws protecting consumer privacy;[122] but the future of California's digital privacy laws is more pertinent to consider given the recent passage of the CCPA.[123] On June 28, 2018, the Governor of California signed the legislation in order to avoid a more restrictive ballot initiative from reaching California voters in November of that year.[124] The original ballot initiative by the same name would not have allowed the legislation to be amended before it was enacted.[125] As a result, the California Legislature jumped into action to create a new bill.[126] The new bill reduces a consumer's opportunity to bring a cause of action.[127] It also "provides flexibility for companies wishing to offer consumer's incentives for their personal data."[128] These changes struck a compromise between citizens who clearly wanted change and the big data industry that may be resistant to such changes, or be unable to implement them quickly.[129]

Even with the changes brought on by the California legislature, the CCPA is the most protective legislation of its kind in the United States. Since the CCPA was passed swiftly, there are still many unanswered questions. To provide some clarification, the California Legislature amended the Act on September 23, 2018.[130] The amendment pushed back the compliance deadline from January 2020 to July 2020.[131] Notably, the amendment also removes the requirement that a consumer notify the Attorney General once a consumer has filed suit under the CCPA.[132] The California Attorney General

122. *See* CAL. BUS. & PROF. CODE § 22575(a) (West 2017) (requiring businesses with websites that collect personal information to "conspicuously post its privacy policy on its Web site"); CAL. CIV. CODE § 1798.83 (West 2009) (requiring companies to inform consumers if their information was being sold for marketing purposes or to allow consumers to opt out). For further discussion of California's protective laws, see Lipman, *supra* note 54, at 793–95, which provides a more detailed analysis.

123. California Consumer Privacy Act, ch. 55, 2018 Cal. Legis. Serv. 1809 (West) (to be codified at CAL. CIV. CODE § 1798.100).

124. Emily Tabatabai et al., *Understanding Calif.'s Game-Changing Data Protection Law: The California Consumer Privacy Act of 2018*, LAW.COM: CORP. COUNS. (July 10, 2018, 5:01 PM), https://www.law.com/corpcounsel/2018/07/10/understanding-calif-s-game-changing-data-protection-law-the-california-consumer-privacy-act-of-2018 [https://perma.cc/J5RV-75CE].

125. Matt Dumiak, *It Passed: The California Consumer Privacy Act of 2018*, COMPLIANCEPOINT (June 29, 2018), http://www.compliancepointblog.com/ccpa/passed-california-consumer-privacy-act-2018 [https://perma.cc/8WCH-4XTQ].

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. Consumer Protection—Privacy, ch. 735, 2018 Cal. Legis. Serv. 4877 (West); *see also* PRACTICAL LAW DATA PRIVACY ADVISOR, CALIFORNIA AMENDS THE CONSUMER PRIVACY ACT OF 2018 (2018), Westlaw W-016-7516 (providing a brief overview of the changes).

131. PRACTICAL LAW DATA PRIVACY ADVISOR, *supra* note 130.

132. California Consumer Privacy Act, ch. 55, § 3, 2018 Cal. Legis. Serv. 1809, 1823 (West) (to be codified at CAL. CIV. CODE § 1798.150(b)). For an overview of the amendments, see JONES

solicited public input on the CCPA.[133] The first input will be used to draft Regulations to clarify how the CCPA will be enforced and provide guidance for businesses on how to comply.[134]

The California legislature amended the CCPA again in September of 2019.[135] One of the amendments seeks to regulate data brokers specifically.[136] The CCPA "define[s] a data broker as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[137] The data broker amendment requires data brokers to register with the California Attorney General or face potential fines.[138] It also requires that the Attorney General create a publicly available registry of the data brokers.[139] This amendment is an important step toward protecting California consumers' privacy, especially considering the fact that data brokers were not previously addressed in the CCPA at all. Allowing consumers to see the companies that collect their data is vital.

The CCPA provides an expansive definition of "personal information."[140] The Act covers more conventional identifiers such as name, email address, social security number, etc.[141] The CCPA also includes forms of identification one may not have considered, such as electronic browsing data, geolocation, purchasing history, IP address, and biometric information.[142] Also protected are "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[143] Such an expansive definition of "personal information" should greatly protect California consumers. The September 2018 amendment provided clarification that "personal information" constitutes data "that identifies,

---

DAY, CALIFORNIA CONSUMER PRIVACY ACT GUIDE 17 (2018), *available at* https://www.jdsupra.com/legalnews/california-consumer-privacy-act-guide-13463 [https://perma.cc/XS8C-X3CV].

133. Brian H. Lam, *California AG's Office Gets Public Input on CCPA*, NAT'L L. REV. (Jan. 29, 2019), https://www.natlawreview.com/article/california-ag-s-office-gets-public-input-ccpa [https://perma.cc/9UW3-YWBV].

134. *Id.*

135. For a comprehensive rundown of the amendments, see Helen Goff Foster et al., *Final CCPA Amendments Awaiting Governor's Signature—and a New Ballot Initiative Is in the Works*, JD SUPRA (Sept. 26, 2019), https://www.jdsupra.com/legalnews/final-ccpa-amendments-awaiting-governor-96825 [https://perma.cc/69DL-MFJF].

136. Assemb. B. 1202, 2019 Gen. Assemb., Reg. Sess. (Cal.) (to be codified at CAL. CIV. CODE § 1798.99.80).

137. *Id.*

138. *Id.*

139. *Id.*

140. California Consumer Privacy Act § 3, at 1818 (to be codified at CAL. CIV. CODE § 1798.140(o)(1)).

141. *Id.* (to be codified at CAL. CIV. CODE § 1798.140(o)(1)(A)).

142. *Id.* at 1818–19 (to be codified at CAL. CIV. CODE § 1798.140(o)(1)(A)–(K)).

143. *Id.* at 1819 (to be codified at CAL. CIV. CODE § 1798.140(o)(1)(K)).

relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[144]

Not only does the CCPA provide broad protection from an information standpoint, it also governs a wide variety of entities. The CCPA defines "business" as:

> A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and . . . determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of [$25 million] . . . (B) . . . buys, receives . . . , sells, or shares for commercial purposes . . . the personal information of 50,000 or more consumers, households, or devices[; or] (C) [d]erives 50 percent or more of its annual revenues from selling consumers' personal information.[145]

This expansive definition of a "business" for purposes of the CCPA provides further evidence of California's serious intent to protect its consumers' digital privacy.

One major regulation is the CCPA's opt-out provision. Under the opt-out provision, a consumer has the right "to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[146] The Act also assures that consumers will know about this right because it requires a business to have a web page entitled "Do Not Sell My Personal Information."[147] A web page with such an eye-catching title is sure to grab the attention of a consumer. This provision will shed some light on the market for consumer data and provide consumers with redress they did not formerly have.

2. Vermont Directly Regulates Data Brokers

Another state that has taken initiative to protect consumer data, specifically data acquired by data brokers, is Vermont. In May of 2018, Vermont enacted the first law in the United States focused exclusively on regulating data brokers.[148] The Act broadly defines "data broker" as "a

144. *Id.* at 1818 (to be codified at CAL. CIV. CODE § 1798.140(o)(1)).

145. *Id.* at 1816–17 (to be codified at CAL. CIV. CODE § 1798.140(c)(1)); *see also* Tabatabai et al., *supra* note 124.

146. CAL. CIV. CODE § 1798.120(a) (West Supp. 2019) (effective Jan. 1, 2020).

147. *Id.* § 1798.135(a)(1) (effective Jan. 1, 2020).

148. Hunton Andrews Kurth, *Vermont Enacts Nation's First Data Broker Legislation*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SECURITY L. BLOG (June 13, 2018), https://www.hunton

business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."[149] This definition assures that the regulation will be far reaching.

The Act defines "brokered personal information" as one may expect, including items such as name, address, date of birth, etc.[150] It also protects biometric data and "other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty."[151] It is worth noting that the legislation does not include browsing history or inferred characteristics in its definition of personal information. The legislature may have intended "other information" be a catchall provision that includes such data.

The Act goes on to require data brokers to register with the secretary of state by January 1, 2019, and pay a registration fee of $100.[152] It also requires data brokers to disclose information about their practices, including whether the brokers provide a method for opting out, and if so, what that process looks like.[153] In addition to registering, data brokers are required to develop security measures in accordance with the legislature's standards.[154] The Attorney General for Vermont praised the legislation and characterized it as a step in the right direction towards protecting consumers within the state.[155]

D. EUROPEAN PRIVACY LAWS AND DATA BROKERS

The EU has a long history of protecting its citizens' private data. In the 1950s, the Convention for the Protection of Human Rights and Fundamental Freedoms recognized a fundamental right to privacy.[156] In the years that followed, several Member States of the EU adopted their own data privacy laws.[157] In 1995, the European Parliament passed the EU Data Protection

privacyblog.com/2018/06/13/vermont-enacts-nations-first-data-broker-legislation [https://perma.cc/XV3K-76GG].

149. Act of May 22, 2018, no. 171, § 2, 2018-3 Vt. Adv. Legis. Serv. 515, 518 (LexisNexis) (codified at VT. STAT. ANN. tit. 9, § 2430(4)(A) (Supp. 2018) (effective Jan. 1, 2019)).

150. *Id.* (codified at VT. STAT. ANN. tit. 9, § 2430(1)(A)).

151. *Id.* (codified at VT. STAT. ANN. tit. 9, § 2430(1)(A)(ix)).

152. *Id.* at 521 (codified at VT. STAT. ANN. tit. 9, § 2446 (a)(1)–(2)).

153. *Id.* (codified at VT. STAT. ANN. tit. 9, § 2446(a)(3)(B)).

154. *Id.* at 522 (codified at VT. STAT. ANN. tit. 9, § 2447) (detailing the various security measures expected of data brokers).

155. Press Release, Chris Curtis, Chief of Pub. Prot., Office of the Attorney Gen., A.G.: New Data Broker Law Is Good for Vermonters (May 24, 2018), *available at* http://ago.vermont.gov/blog/2018/05/24/a-g-new-data-broker-law-is-good-for-vermonters [https://perma.cc/ZXB4-RV6M].

156. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, 230 ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

157. FRANÇOISE GILBERT, GLOBAL PRIVACY AND SECURITY LAW § 4.06 (Supp. 2019).

Directive.[158] The Directive was created "to harmonize the existing laws and pave the way for the upcoming laws to be drafted."[159] The Directive did just that, serving as a jumping off point for subsequent legislation. The Directive provided sweeping protections for citizens, as well as vocabulary that would be used in later regulations.[160]

The EU built upon the Directive to create the innovative General Data Protection Regulation ("GDPR"). The GDPR went into effect on May 25, 2018.[161] It provides expansive protections to citizens of the EU regarding their online privacy and broadly regulates businesses that retain and process data in the EU.[162] The GDPR imposes regulations on both "data controllers"[163] and "data processors."[164] The Regulation also carries the threat of massive fines for noncompliance.[165] Considering the entities governed by the GDPR, data brokers likely fall into the data processor category.

The GDPR requires a strong line of communication between data processors and data controllers.[166] These entities must have a "lawful purpose" (or a lawful basis) for collection and processing of data.[167] Additionally, such organizations must keep records of their compliance in case the company is audited.[168] The GDPR also requires that entities provide citizens with information about their practices and reasons for collecting data.[169]

The GDPR provides EU citizens with a host of protections. It defines "personal data" as:

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

158. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

159. GILBERT, *supra* note 157, § 6.01.

160. *Id.*

161. IT GOVERNANCE PRIVACY TEAM, EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE 1 (2d ed. 2017).

162. *Id.*

163. Data controllers are defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." General Data Protection Regulation 2016/679, art. 4, cl. 7, 2016 O.J. (L 119) 33 (EU).

164. Data processors are defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.* art. 4, cl. 8, at 33.

165. *Id.* art. 83, cl. 5, at 83 ("[A]dministrative fines of up to 20[,]000[,]000 [Euro], or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher . . . .").

166. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 235–39. The GDPR also sets out contractual requirements in Article 28. *Id.* at 238.

167. General Data Protection Regulation 2016/679, art. 5, 2016 O.J. (L 119) 35–36 (EU).

168. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 242.

169. *Id.* at 242–44.

> data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[170]

Data subjects are "entitled to know what personal data of theirs is being processed, the lawful basis of that processing, as well as whether or not their personal data is being processed by the controller or by a third-party processor."[171] These provisions mean that data subjects will know if their data will be sold to a third-party entity such as a data broker. In order to prevent companies from hiding behind convoluted legalese, the GDPR requires the data subject be provided notice "in a concise, transparent, intelligible and easily accessible form, using clear and plain language."[172]

In addition to providing notice of data collection and processing, organizations must get consent from consumers in order to process their data.[173] The consent must be given "freely" and must be "informed and unambiguous."[174] In order to reach this threshold, organizations must provide a "genuine option [to] refus[e]" without consequences.[175] Furthermore, the data subject may "withdraw [their] consent at any time."[176] The GDPR enables the data subject to have substantial control over their data, to be well informed about where their data is going, and how the data will be used. To illustrate consent in the GDPR, imagine loaning someone your vehicle to go to a gas station and you see on social media that they are out on the town. You would revoke the privilege of using your car. Consent in the GDPR is similar: If a company is using your data in a way that you did not consent to, you have the right to revoke that consent.

Since the GDPR is rather new, it is unclear precisely how it will affect data brokers. From the structure of the regulations, it appears data brokers will no longer be able to collect information directly from data subjects in the EU without their knowledge. Presumably, data brokers will be at the mercy of various data controllers for the information they need. Such controllers must make it clear to data subjects that a third party will process the information. If a data subject does not consent, the data broker will not be able to process the information. Such a situation seems quite likely if the data subject has no incentive to permit the processing of their data by a third party.

---

170. General Data Protection Regulation 2016/679, art. 4, cl. 1, 2016 O.J. (L 119) 33 (EU).
171. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 188.
172. General Data Protection Regulation 2016/679, art. 12, cl. 1, 2016 O.J. (L 119) 39 (EU).
173. *Id.* art. 7, at 37.
174. *Id.* art. 4, cl. 11, at 34.
175. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 206.
176. General Data Protection Regulation 2016/679, art. 7, cl. 3, 2016 O.J. (L 119) 37 (EU).

III. CONSUMERS IN THE UNITED STATES NEED PROTECTION FROM THE HIGHLY EVASIVE AND INVASIVE PRACTICES OF DATA BROKERS

Data brokers are particularly problematic because they collect a vast array of consumer information largely without consumer knowledge. If consumers are not aware that their data is being collected nearly every time they transact, they are unable to protect themselves. In a "first-of-its-kind empirical study" on online privacy attitudes, conducted at the University of Illinois at Urbana-Champaign ("UIUC"), 89 percent of participants indicated that they did not think marketing and advertising companies should be permitted to "track consumers' online activity without asking for permission."[177] Even if consumers are aware that their activities are being tracked and stored, they may not feel they have a meaningful choice to decline sharing information. This is evidenced by the 81 percent of participants in the same study that indicated they had shared "information online when they wished they [had] not."[178] Entities such as Internet service providers, advertising agencies, and search engines ranked very low in consumer trust regarding protecting their personal data.[179]

Entities that collect and sell consumer data often provide their consumers with convoluted information about their practices. Consumers frequently agree to a Terms of Service ("ToS") agreement in order to use a web page or an app. The terms in a ToS agreement usually detail "what information will be collected" and whether it may be sold.[180] Most consumers (understandably) do not read these agreements.[181] The UIUC study found that when asked why they do not read the ToS, the majority of consumers said they were too long.[182] One consumer pointed out that reading the ToS is futile

177. Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 297 & tbl.1 (2016).

178. *Id.* at 343. According to the researchers in that study:

> There are many possible explanations for this. First, they may do this because they believe that the benefits of using the service outweigh the downsides of using the service. Or they may believe that the benefits from using the service are greater than the benefits from *not* using the service. Another possible explanation is that the consumers do not know enough to make meaningful decisions about their online privacy. In the alternative, maybe consumers know enough but feel helpless to make a decision that differs from what companies are willing to offer.

Id. Regardless of the reason why consumers feel this way, that number is staggering.

179. *Id.* at 301–02.

180. *Id.* at 285.

181. *Id.* at 288–89. Consumer actions regarding ToS are understandable when one considers that "[i]f people did suddenly start reading privacy policies and TOS agreements, . . . the national opportunity costs could potentially be very high, perhaps into the hundreds of billions of dollars, considering how many websites the average user visits every year and how many hours would be required." *Id.*

182. *Id.* at 295.

if one wants to use the service that a website or app provides.[183] According to the UIUC study, less than half of participants had decided not to use a website because of the ToS agreement.[184] Despite this finding, "92% of respondents somewhat or strongly agreed with the statement, 'Personal privacy is important to me.'"[185]

Big data companies are able to continue these practices because consumers see no other way out if they wish to enjoy online services. Consumer information is extremely valuable.[186] Currently, big data companies are arguably the only ones benefitting from the commodification of information. Consumers browse and purchase on the web freely in exchange for sharing these activities with an unknown number of entities. This exchange is unequal, and it is unfair.

Without knowledge of where their information might go, consumers are unable to protect their individual privacy interests. Consumers are often unaware that their information often ends up in the hands of data brokers. For many years, data brokers have been profiting billions of dollars on consumer information, largely operating without regulation or consumer knowledge.[187] Data brokers fundamentally lack transparency regarding their practices.[188] Such a lack of transparency exacerbates consumer skepticism about the big data industry.

Data brokers not only pose a risk to consumers regarding lack of consumer knowledge, but there is also concern about discrimination resulting from their practices. Consumers are categorized into data segments, many of which may be harmless;[189] however, if an individual is categorized as "low income," they may be subject "to ads for subprime credit or receiving different levels of service from companies."[190] Similarly, an insurance company could categorize someone placed in a "Diabetes Interest" segment as a high-risk individual.[191] If the consumer does not know why they are receiving such targeted ads, they are unable to mitigate this harm.

---

183. *Id.* ("There's nothing I can do about it if I want to use their services.").

184. *Id.*

185. *Id.* at 296. The disparity between consumer attitudes about privacy being important to them while not reading privacy policies is cause for concern. It means that individuals are compromising on something that is important to them without fully considering the consequences.

186. *See generally* Julia N. Mehlman, Note, *If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information: A Look at the Data-Collection Industry and a Proposal for Recognizing the Value of Consumer Information*, 81 BROOK. L. REV. 329 (2015) (detailing the data broker industry and emphasizing the value of consumer information).

187. Glasgow, *supra* note 15, at 25–26.

188. RAMIREZ ET AL., *supra* note 18, at 49.

189. *Id.* at 19, 47–48.

190. *Id.* at 48.

191. *Id.*

This potential for discrimination is especially concerning when one considers the fact that brokered information is often inaccurate.[192] Imagine an individual is categorized as having children, but she does not, and she seeks employment somewhere that is not family friendly. This individual could be passed over for the job if the potential employer gets inaccurate information. Setting aside the other issues in this scenario, it is unfair that the individual would be rejected because of inaccurate information. The individual would have no way of knowing that misinformation is why she was rejected and would not be able to rectify the issues. Potential discrimination and lack of transparency are huge issues brought on by the data broker industry.

Another concern related to the data broker industry is the potential for data breaches. Most people are familiar with breaches of large, consumer-facing companies such as Facebook.[193] Likewise, most have heard of the Equifax breach.[194] Data brokers collect and store massive amounts of consumer data, which makes them a target for hackers. Most have never heard of the data broker Exactis, or its data breach of "close to 340 million individual records."[195] Security breaches are a growing problem in today's world. Companies must be proactive in securing information and providing affected consumers with a remedy post-breach. Exactis did not even allow consumers to see if they had been affected.[196]

Brokering consumer data for marketing purposes is a multi-billion-dollar industry that is unregulated in the United States. Although some data brokers have made progress regarding consumer transparency,[197] self-regulation is inadequate for such a large industry handling potentially sensitive information about consumers. An attempt at organized self-regulation in the data broker industry failed in the 1990s.[198] Today, there are other entities that provide guidelines for digital advertising and data collection.[199] None of these

192. *See supra* Section II.A.1.

193. Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html [https://perma.cc/CS2S-S3UF].

194. Seena Gressin, *The Equifax Data Breach: What to Do*, FTC: CONSUMER INFO. BLOG (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/GL4Z-C8RY].

195. Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, WIRED (June 27, 2018, 1:34 PM), https://www.wired.com/story/exactis-database-leak-340-million-records [https://perma.cc/RWT4-MG7H].

196. Ammon Curtis, *The Exactis Breach: 5 Things You Need to Know*, INFOARMOR, https://blog.infoarmor.com/employees/the-exactis-breach-5-things-you-need-to-know [https://perma.cc/8GTX-QWA6] ("Currently, Exactis isn't offering a way to see if you were part of the breach.").

197. *See generally US Consumer Opt Out*, ACXIOM, https://isapps.acxiom.com/optout/optout.aspx [https://perma.cc/E3M2-87MV] (providing consumers with information about how to opt out of having their information collected).

198. RAMIREZ ET AL., *supra* note 18, at vii.

199. Glasgow, *supra* note 15, at 42–43. These entities include the Direct Marketing Association, the Digital Advertising Alliance, and the Network Advertiser's Initiative. *Id.* Each of

entities are focused on regulating data brokers specifically, and of course data brokers are free to choose not to regulate according to their various codes of conduct. Self-regulation in the data broker industry is clearly unpredictable and therefore ineffective. These issues with self-regulation make it clear that some sort of governmental intervention is necessary in order to protect consumer data.

IV. RECOMMENDATIONS FOR FEDERAL LEGISLATION

In order to protect consumer privacy, there must be regulation of data brokers at the federal level. It would be inadequate to let the states handle a matter of national importance such as this on their own. Currently, U.S. citizens' data is vulnerable to hacking due to a lack of adequate security measures. Federal legislation should provide a baseline of protection, and states should be free to provide their citizens with more protection—such as the data broker registry in Vermont. A base level of protection is necessary if the United States is going to take protecting its citizens' digital privacy seriously. Fortunately, the United States does not have to create legislation from scratch. Many provisions and broader concepts found in the GDPR provide a solid foundation upon which the United States can build its own privacy laws.

There are several different solutions that Congress could include in privacy legislation to protect consumers. This Note will now focus on those solutions and explain why they will be effective. Many of the solutions are found in the GDPR, and some have been implemented in California. The first solution would be to implement a meaningful notice-and-choice system, because it would greatly protect consumers by giving them an actual choice in whether to share their data or not. The next thing that Congress should include in privacy legislation is to mandate an option for consumers to have access to and the ability to edit data held by data brokers. This requirement would be helpful both in protecting consumers and providing companies with accurate information. Companies should also make it a point to minimize the amount of data that they require and retain. Another important part of privacy legislation would be strict penalties for noncompliance, which will incentivize companies to take regulation seriously. Finally, creating quasi-governmental entities to assist in regulation will be helpful to all the important individuals in this issue. These entities would provide a trustworthy place for consumers to access and edit their data. Consumer trust will be greater because the government would not run these entities, nor would they be totally in the private market. Creating these entities is vital to the success of regulation of data privacy on the federal level.

---

these entities provides suggested recommendations for best practices for handling consumers' digital information for advertising purposes. *Id.*

A. MEANINGFUL NOTICE-AND-CHOICE OF DATA COLLECTION

Several proponents of digital privacy regulation suggest protecting consumers through a notice-and-choice system.[200] In its report on data brokers, the FTC recommended "Congress should consider requiring consumer-facing entities to provide a prominent notice to consumers that they share consumer data with data brokers and provide consumers with choices about the use of their data."[201] While this recommendation has not been adopted at the federal level, California did follow it. The CCPA states "[a] business that sells consumers' personal information to third parties shall provide notice to consumers."[202] Such a requirement is a positive step toward protecting consumer privacy online.

Though providing notice to consumers about where their information may go is important, in practice it may not be effective. Lengthy ToS agreements are often daunting, and even the most prudent consumer likely will not take the time to read them. According to one study, if a person were to read the privacy policies of the websites she visits in a year, it would take her 244 hours to do.[203] Clearly, reading privacy policies is not a practical thing to do.[204] Even if a layperson attempted to read a lengthy privacy policy, much of the language is convoluted and difficult to understand. There is an apparent need for meaningful notice that provides consumers with actual knowledge of where their information may go and why it may go there.

For some guidance on how to provide meaningful notice, it is helpful to look to the GDPR. Under the GDPR, a data controller must provide notice using "a concise, transparent, intelligible and easily accessible form, using clear and plain language."[205] The GDPR requires entities to provide a broad range of information about data collection.[206] These requirements range

---

200. John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 561–62 (2018). Notice and choice

> requires an information collector to disclose to an individual what personal information it proposes to collect from her and how it proposes to use that information ("notice"), thereby affording the individual an opportunity to prevent the collection of her PII by denying consent or by declining to enter into the transaction ("choice").

Id.

201. RAMIREZ ET AL., *supra* note 18, at viii.

202. Consumer Protection—Privacy, ch. 735, § 5(b), 2018 Cal. Legis. Serv. 4877, 4881 (West) (to be codified at CAL. CIV. CODE § 1798.120). This section of the CCPA points to provisions of the California Civil Code that require notice of the potential sale of personal information and a consumer's right to not sell her information. CAL. CIV. CODE §§ 1798.120(b), 1798.135 (West Supp. 2019).

203. Rothchild, *supra* note 200, at 615–16.

204. *See supra* Part III.

205. General Data Protection Regulation 2016/679, art. 12, cl. 1, 2016 O.J. (L 119) 39 (EU).

206. *Id.* art. 13, at 40–41.

from contact information of the data controller to potential recipients of the data.[207] Providing this information in a clear and concise way is helpful for consumers.[208] In order to provide consumers with clarity regarding the collection and retention of their data, Congress should adopt legislation with notice requirements similar to the GDPR.

Presumably, along with notice of information gathering, there comes a choice about whether to use a particular website or service or not. To choose is defined as "to select freely and after consideration."[209] In the United States, if consumers do not want to share their personal information, companies will likely refuse services to them. This creates a situation where "a consumer's options are either to accept the industry-standard privacy-invasive practices or stay off the Internet."[210] Such drastic consequences for refusing to accept a boilerplate privacy policy that allows for expansive collection and retention of information hardly constitutes a free choice. Entities that collect data must provide a meaningful choice for consumers to not process and share their personal data.

Once again, it is helpful to turn to the GDPR for an example of what providing an adequate choice might look like. The GDPR adopts an "opt-in" method for consumer consent to data processing.[211] This approach means that a consumer must provide "consent to the processing of his or her personal data for one or more specific purposes."[212] The consent requirement is stringent.[213] A company must "ensure that the data subject has the genuine option of refusal, and that there will be no repercussions for refusing to consent."[214] If an entity that processes information cannot meet this requirement, it must provide a "valid legal basis" for processing the information anyway.[215] The GDPR stipulates that consent and free choice are examined carefully.[216] This opt-in method with a critical view toward consent

207. *Id.*

208. *Compare* Ben Davis, *GDPR: How to Create Best Practice Privacy Notices (With Examples)*, ECONSULTANCY (July 17, 2017), https://econsultancy.com/gdpr-best-practice-privacy-notices-examples [https://perma.cc/LMD6-EKPS] (providing helpful examples of appropriate notices), *with Privacy Policy and Your Privacy Rights*, L.A. TIMES: PRIVACY POLICY, http://www.latimes.com/about/la-privacypolicy-20180703-story.html [https://perma.cc/8BMF-PPJE] (last updated June 19, 2018) (detailing the privacy policy of the L.A. Times, which withdrew from providing services in the EU as opposed to attempting GDPR compliance). For an example of a presumably GDPR-compliant privacy policy, see *Privacy Policy*, PINTEREST, https://policy.pinterest.com/en/privacy-policy [https://perma.cc/CA3W-B8EG] (last updated June 28, 2019).

209. *Choose*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/choosing [https://perma.cc/V6Z2-38WH].

210. Rothchild, *supra* note 200, at 627.

211. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 206–07.

212. General Data Protection Regulation 2016/679, art. 6, cl. 1(a), 2016 O.J. (L 119) 36 (EU).

213. *See supra* Section II.D.

214. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 206.

215. *Id.*

216. General Data Protection Regulation 2016/679, art. 7, cl. 4, 2016 O.J. (L 119) 37 (EU).

is the best way to protect a consumer's choice about whether to share his or her data. Congress should adopt legislation with similar requirements.

Some argue that an opt-out method serves just as well as opt-in. In fact, one way the CCPA differs from the GDPR is that it provides an opt-out method.[217] Under this method, consent to information processing is assumed—as it is currently. If an individual decides he or she no longer wishes to share his or her information, the individual has the option to opt-out of information sharing. The opt-out method is better than the current U.S. regime, where companies are free to decide whether to allow individuals to opt-out or not; however, it does not provide the utmost protection to the consumer. There is a chance a consumer will be unaware of his or her right to opt-out, leaving the consumer in the same position he or she would be in if there were no regulation. The opt-in method is preferable because a consumer will not be confused about his or her rights. Under an opt-in method, consumers have full autonomy over their personal data and a meaningful choice about whether to share their information or not.

In addition to the opt-in model that requires consumer consent on the front end, consumers should also be able to withdraw consent at any time. Under the GDPR, European citizens have an absolute right to refuse to have their personal data collected for direct marketing purposes.[218] This absolute right means that if a company receives a request from a consumer to quit processing his or her data, the company must comply.[219] Providing consumers with the right to object to the processing of their personal information is important to preserving their right to a free choice.

An opt-in requirement for the processing of personal data is preferable in the United States because it provides consumers with a meaningful choice about whether to share their information with companies or not. Consumers should not face any repercussions such as refusal of services if they choose not to share their data. If consumers do decide to share their data, they should be free to opt out at any time. Borrowing some language from the GDPR, a U.S. notice and choice provision could read as follows:

> Processing data shall only be lawful if a data subject consents to such processing. Data processors must put a data subject on notice that their information is being collected and for what purpose.

---

217. Consumer Protection—Privacy, ch. 735, § 5(b), 2018 Cal. Legis. Serv. 4877, 4881 (West) (to be codified at CAL. CIV. CODE § 1798.120).

218. General Data Protection Regulation 2016/679, art. 21, cl. 2, 2016 O.J. (L 119) 45 (EU). The relevant provision reads, "[w]here personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing." *Id.*

219. *Right to Object*, INFO. COMMISSIONER'S OFF. (Aug. 2, 2018), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object [https://perma.cc/BGU3-6G2G].

> Furthermore, the data processor must make it explicitly clear that collected information may be sold to third parties. Such notice must be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Furthermore, a data processor shall provide a genuine option for refusal without negative repercussions. A data subject shall have the right to withdraw any consent given at any time.[220]

Such a provision would provide meaningful notice to a consumer that her data may be collected and provide the choice about whether to allow such collection. Furthermore, such a consumer would be free to opt out of sharing at any point.

B. PROVIDE CONSUMERS WITH THE OPTION TO EDIT THEIR DATA

Another important way to provide consumers with autonomy over their data is to give them the right to edit any inaccurate data. Data brokers often have inaccurate information.[221] This was true for the author of this Note.[222] Inaccurate information may have harmful discriminatory effects on consumers.[223] Less concerning, but still relevant, is that inaccurate information may also lead to receiving targeted marketing unrelated to consumer interests. This could cause serious reputational harm to individuals, and it creates unnecessary costs for companies paying for marketing services.

In order to allow consumers to edit incorrect information about them, they must have access to that information. It is currently at the data broker's discretion whether to allow consumers access to their information.[224] In the FTC report on data brokers, only four of the nine companies allowed consumers to access limited information about themselves.[225] It is wholly up

---

220. *See supra* notes 200–19 and accompanying text.

221. *See supra* Section II.A.1; *see also* Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data—But They Got Me Wildly Wrong*, FORBES (Apr. 5, 2018, 4:08 PM), https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/#33329f853107 [https://perma.cc/BA43-LLZ2] (detailing one journalist's experience accumulating information from several data brokers about himself that was inaccurate and difficult to acquire).

222. Out of curiosity, I visited Acxiom's aboutthedata.com and made an account. Acxiom had my birthday and my gender correct, but it said that I am married with one child. I am neither married nor do I have a child. Acxiom had information about how much money I spend both off and online. Under the "interests" heading, some of them were accurate such as "fashion" and "reading," but others were not, for instance "PC Owner" and "Hunting/Shooting." It was interesting to see my own information in Acxiom's database. I had the option to correct Acxiom's errors, or to opt-out of having my information used by them for marketing purposes. The website was overall very helpful and user-friendly. It is clear from the website's layout and the options it provides that Acxiom intends to be an industry leader in fostering trust between the data broker industry and consumers.

223. *See supra* Part III.

224. *See* RAMIREZ ET AL., *supra* note 18, at 42.

225. *Id.*

to a data broker to determine what information it wants to share with the consumer.[226] In order to access their information, consumers must provide documentation to prove their identities.[227] Companies may request these documents by potentially unsafe means.[228] Basic fairness requires that individuals should have access to information companies are keeping about them. Access to information about one's self is important. It is also vital that if consumers detect an inaccuracy in the information a company has on them, then they are able to rectify the mistake.

The best way to protect both consumers and businesses is allowing consumers to access and edit the data companies have about them. Currently it is at the data broker's discretion whether or not it will allow consumers to edit their information.[229] According to the FTC study of nine data brokers, only two "allow[ed] consumers to correct their information."[230] This makes little sense given the fact that consumers are in the best position to provide accurate information and one would expect these large data aggregation entities to want accurate information. Data brokers may be concerned that if consumers have more control over their data, they may be less likely to share their information, but there is evidence to suggest that the opposite is true.[231] Providing consumers with the right to edit their data is beneficial both to the consumer and the businesses collecting information from the consumer.

Congress should follow the GDPR's model regarding access to information and the ability to edit that information. Regarding access to information, data controllers should be required to provide data subjects with access to "a copy of their personal data, the purposes of processing their data, the categories of the data being processed, and the third parties or categories of third parties that will receive their data."[232] Additionally, this information should "be provided free of charge"[233] within one month after the request for access is received.[234] Data controllers should be required to verify the identity of the data subject in order to release the information;[235] however, the data controller should not be able to retain information given specifically for

226. *Id.*

227. *Id.*

228. *See* Leetaru, *supra* note 221 (detailing how one data broker, Oracle, told him to send either his passport or ID to them via unencrypted email).

229. RAMIREZ ET AL., *supra* note 18, at 42.

230. *Id.*

231. Kesan et al., *supra* note 177, at 351.

232. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 190 (footnote omitted); *see also* General Data Protection Regulation 2016/679, art. 15, cl. 1, 2016 O.J. (L 119) 43 (EU).

233. General Data Protection Regulation 2016/679, art. 12, cl. 5, 2016 O.J. (L 119) 40 (EU).

234. *Id.* art. 12, cl. 3, at 40. The GDPR does provide an exception to extend the deadline to two months if the request is complex, but the data controller must inform the data subject about the delay and the reason for it. *Id.*

235. IT GOVERNANCE PRIVACY TEAM, *supra* note 161, at 228–29.

identification purposes.[236] California included similar provisions in the CCPA.[237] These requirements should be adopted in the United States to provide individuals with access to their information. Additionally, data controllers should take appropriate measures to ensure that proof of identity is properly secured. Consumers should be able to prove their identity and have access to their information safely. They should not be in the dark about what information certain companies have on them. Borrowing from the GDPR, such a provision in data privacy legislation could read as follows:

> Data subjects shall have the right to obtain a copy of their personal data, the purposes for processing their data, the categories of data being processed, and the third parties or categories of third parties that will receive their data. Furthermore, the data subject shall be permitted to rectify any inaccuracies in the information or fill in missing properties. Data subjects shall be provided access to their requested data within thirty days, free of charge to the data subject, and any requested edits to the data should be made promptly after the request is made.[238]

Such a provision would provide U.S. consumers with meaningful access to their data.

If consumers have access to their information, they may identify that some information is incorrect and should be provided the right to correct inaccuracies. The GDPR provides a "right to rectification."[239] Under this right, "[t]he data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her."[240] Congress should follow this model of allowing consumers to edit their information quickly. If Congress were to adopt access and editing rights similar to that of the GDPR, it would greatly increase transparency between consumers and the data broker industry. Consumers will have more peace of mind knowing that they are able to access and edit large quantities of information about themselves. Data brokers and other companies that collect data will also benefit from increased accuracy of information.

C. DATA MINIMIZATION

Another way to protect consumer information is to forbid companies from acquiring more than necessary. Data minimization is "the practice of limiting the collection of personal information to that which is directly

236. *Id.*

237. Consumer Protection—Privacy, ch. 735, § 5(a)–(b), 2018 Cal. Legis. Serv. 4877, 4881 (West) (to be codified at CAL. CIV. CODE § 1798.120).

238. *See supra* notes 224–37 and accompanying text.

239. General Data Protection Regulation 2016/679, art. 16, 2016 O.J. (L 119) 43 (EU).

240. *Id.*

relevant and necessary to accomplish a specified purpose."[241] Currently, there are no limits to the amount of information that a data broker may collect and store.[242] Data brokers have free reign over vast amounts of consumer information and some of this information may be personal. Data brokers collect an obscene amount of consumer information.[243] They also may save outdated or incorrect information.[244] It is unlikely that all this information is absolutely necessary to carry out business purposes. For this reason, Congress should implement data minimization into data privacy legislation.

The GDPR provides guidance about what a data minimization requirement should look like. Under the GDPR, personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[245] Limiting the amount of data a company can obtain and retain may protect the company from breaches.[246] Additionally, it will save companies money, given the fact that data storage is expensive.[247] Data brokers may balk at the idea of data minimization because their entire business revolves around aggregation of data, but they should not overlook the benefits of limiting data storage. It is also important for data brokers to recognize that some of the information they are storing is no longer relevant, and therefore no longer valuable.[248] Regarding necessity, it is not necessary to keep credit card information if a company is analyzing purchasing trends.[249] Ultimately, limiting the amount of information an entity may collect about a consumer protects both the consumer and the entity collecting the information.

D. STIFF PENALTIES FOR FAILURE TO COMPLY

One reason the GDPR will likely see great success regarding compliance is its hefty fine structure. Violators of the GDPR will "be subject to administrative fines up to 20[,]000[,]000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."[250] With such extreme fines, it

241. Bernard Marr, *Why Data Minimization Is an Important Concept in the Age of Big Data*, FORBES (Mar. 16, 2016, 3:24 AM), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data [perma.cc/WE2V-LFLR].

242. RAMIREZ ET AL., *supra* note 18, at 22.

243. *Id.* at 14 ("One data broker that compiles . . . information maintains data of over 240 million consumers sorted into 1000 interest categories.").

244. *Id.* at 48–49.

245. General Data Protection Regulation 2016/679, art. 5, cl. 1(c), 2016 O.J. (L 119) 35 (EU).

246. Marr, *supra* note 241.

247. *Id.*

248. JT Sison, *Data Minimization in the GDPR: A Primer*, DATAGUISE: BLOG (Feb. 15, 2017), https://www.dataguise.com/gdpr-compliance-data-minimization-use-purpose [https://perma.cc/BNF4-SMC2].

249. *Id.*

250. General Data Protection Regulation 2016/679, art. 83, cl. 5, 2016 O.J. (L 119) 83 (EU).

is no wonder that the GDPR has been widely discussed and many companies are seeking consultation on how to comply. Regulatory entities called Data Protection Authorities are charged with enforcing the GDPR.[251] For example, the Information Commissioner's Office is an independent regulatory office in charge of enforcing the GDPR in the United Kingdom.[252] The first fine under the GDPR was issued "to Google for failing to comply with [the] GDPR[;]" the company will have to pay 50 million Euros.[253] While the fine is not the maximum amount that it could have been, the fine sends a message to entities that collect data all over the world that the EU is serious about the GDPR and its citizens' right to privacy.

In order to assure similar success, the United States should impose severe penalties for failing to comply with privacy legislation. Without large fines, big data companies will likely continue whatever detrimental practices they are participating in and opt to pay a smaller fine. If the United States imposes strict fines, it will also show companies collecting information from United States citizens that they must take great care in doing so. Furthermore, if the United States joined the EU in imposing stringent regulation of digital privacy paired with strict consequences, it would greatly increase digital privacy on a global scale.

E. CREATION OF AN ENTITY TO ASSIST IN REGULATION

Another solution to protect consumers' online data does not come from the GDPR; rather, it is a recommendation following an empirical analysis on consumer attitudes toward digital privacy.[254] The recommendation suggests that the best way to protect consumer privacy in a way consumers will trust is through a third party entity.[255] After the creation of extensive data privacy legislation on the federal level, "profile repositories" would be created to "allow consumers to manage their profile information as used for marketing purposes."[256]

These repositories would be called Profile Information Reporting Agencies ("PIRAs").[257] This "market-based clearinghouse solution" is ideal

251. *What Are Data Protection Authorities (DPAs)?*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [https://perma.cc/73U9-K6CX].

252. *The Role of the Information Commissioner's Office (ICO) in Relation to the GDPR*, KEFRON: BLOG, https://www.kefron.com/blog/role-of-the-information-commissioners-office [https://perma.cc/JQU9-GTWA].

253. Emily Price, *France Fines Google $57 Million for GDPR Violations*, FORTUNE (Jan. 21, 2019), http://fortune.com/2019/01/21/france-fines-google-57-million-for-gdpr-violations [https://perma.cc/SMG4-GA3G].

254. For more on the results of this extensive study, see generally Kesan et al., *supra* note 177 (polling consumers on many different aspects of consumer privacy and data security).

255. *Id.* at 346.

256. *Id.*

257. *Id.*

considering low consumer trust in the government handling their data.[258] Although the government would not be handling consumer data, it would provide a valuable oversight role.[259]

The structure of PIRAs would follow the model set forth in one of the current sector-specific privacy laws—the Fair Credit Reporting Act ("FCRA").[260] The FCRA "provides directions and limits on how credit reporting companies disclose credit report information."[261] Some of these limitations include the right to access one's credit report and to dispute inaccurate information.[262] The FCRA provides oversight that "arguably helps ensure that the private companies providing credit reporting services can build and maintain the public's trust."[263] The model of the FCRA and its oversight of credit reporting agencies provide an ideal framework for PIRAs.

In addition to the other suggestions in this Note, this legislation should also "recommend the initial organization of PIRAs."[264] The government could incentivize companies to become PIRAs by providing subsidies.[265] The legislation would also need to "provide guidelines concerning the situations when a consumer's profile information can be shared with entities other than the consumer."[266] Once established, "PIRAs would provide a location where an individual consumer could register and view aggregated profile

---

258. *Id.* at 346–47. The researchers in the UIUC Study echoed many of the sentiments in this Note regarding digital privacy reform:

> After conducting a detailed survey to examine knowledge, opinions, and behaviors regarding online privacy, it appears likely that privacy regulations will be met with skepticism if adequate controls are not assured. Participants in our survey seem to want to be involved in the choices made about their data, but the current paradigm makes this difficult. To this end, data privacy legislation should emphasize a two-part approach. Consumers should be assured that their information will be shared only with their consent through an opt-in system, and they should also have the ability to view, challenge, and remove this information. This increase in transparency is likely to lead to an increase of trust and thus move the consumer's relationship with data holders from complacency to consent.

Id. at 347.

259. *Id.*

260. *Id.*; 15 U.S.C. § 1681 (2012).

261. *What Is a Credit Reporting Company?*, CONSUMER FIN. PROTECTION BUREAU, https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-reporting-company-en-1251 [https://perma.cc/EE8C-LFA7] (last updated Jan. 31, 2018). For more about individual rights under the FCRA, see CONSUMER FIN. PROT. BUREAU, A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (2014), *available at* https://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf [https://perma.cc/PW75-LPHE] [hereinafter CONSUMER FIN. PROT. BUREAU, A SUMMARY].

262. CONSUMER FIN. PROT. BUREAU, A SUMMARY, *supra* note 261.

263. Kesan et al., *supra* note 177, at 347.

264. *Id.*

265. *Id.*

266. *Id.*

information about herself."[267] In the same portal, a consumer could also challenge misinformation or remove some information entirely.[268] PIRAs would provide an avenue for protecting consumer information without a great burden to either the government or data collectors themselves. The system would also create helpful and accurate repositories where data brokers could potentially acquire accurate information. Legislation on the federal level and the creation of PIRAs would provide the ultimate protection of digital consumer data.

V. CONCLUSION

Regulation of data brokers on the federal level is vital to protect consumer data online. The United States' current approach to data privacy laws is insufficient to regulate the use of consumer information, particularly for marketing purposes. The GDPR has provided excellent guidelines for data privacy legislation moving forward. California and Vermont have taken matters into their own hands by passing their own legislation. Congress should follow this leadership and pass legislation to protect consumer privacy online. This legislation should include a meaningful notice-and-choice system that would protect consumers by giving them an actual choice about whether to share their data or not. An option for consumers to have access to and the ability to edit data held by data brokers would also be helpful in protecting consumers and providing companies with accurate information. Requiring companies to minimize the amount of the data they collect and retain will also help to protect consumer data from the risk of breach. Strict penalties for noncompliance will assist in companies taking regulation seriously. Finally, creating quasi-governmental entities to assist in regulation will be helpful to all the important players in this equation. Each of these solutions should be included in federal legislation to protect consumers' digital privacy.

---

267. *Id.* at 348.

268. *Id.* There are sound reasons to employ this model, which the UIUC study articulated well:

> One of our arguments for giving consumers the ability to view, challenge, and remove data from their profile is an ethical one. Consider, for example, a woman who desires to become a mother, but who has had many miscarriages. One of the most profitable markets is pregnant women and mothers, and she likely has been considered part of this market ever since her first purchase of prenatal vitamins. For this individual, an endless stream of advertisements about pregnancy and children is not only ineffective for the advertiser, it is cruel to the target. PIRAs would allow her to remove aspects of her profile that could trigger emotional distress, giving her the freedom to choose how she represents herself.

Id.