Florida State University Law Review

Volume 45 | Issue 1 Article 6

Fall 2017

Guardians of the Galaxy of Personal Data: Assessing the Threat of Big Data and Examining Potential Corporate and Governmental Solutions

Timothy A. Asta

GUARDIANS OF THE GALAXY OF PERSONAL DATA: ASSESSING THE THREAT OF BIG DATA AND EXAMINING POTENTIAL CORPORATE AND GOVERNMENTAL SOLUTIONS

TIMOTHY A. ASTA*

* J.D., 2017, Florida State University College of Law. Special thanks to my wife, Heather McLellan Asta, for all of her support.

> *Relying on government to protect your privacy is like asking a peeping tom to install your window blinds.*[1]
>
> —John Perry Barlow

> *In the end, if the people cannot trust their government to do the job for which it exists to protect them and to promote their common welfare—all else is lost.*[2]
>
> —Barack Obama

I. INTRODUCTION

Take a moment to visit one of the following websites: Spokeo.com,[3] PeopleLookup.com,[4] PrivateEye.com,[5] or, if time is of the essence, PublicRecordsNOW.com.[6] Type in your name and look at the results. What you will find is not just the result of the website query, but in fact the outcome of modern big data collection and analytics. The aggregation of personal information presents unique and often amorphous threats to personal privacy,[7] potential harms that the protections guaranteed by the U.S. Constitution (as interpreted by the U.S. Supreme Court) appear insufficient to guard against.[8] Perhaps corporations, not the government, would be more effective at ensuring the fidelity and security of consumer information. Corporate actions and public statements over the past few years would suggest that corporations are eager to take on the mantle of data protection and crown themselves guardians of our personal data. For example, in February 2016, following the mass shooting attack in San Bernardino, California, Apple refused to comply with an official order from the Federal Bureau of Investigation (FBI) to unlock one of the suspected perpetrators' iPhones—an action which, in Apple's view, risked the privacy and security of its customers, including tens of millions of Americans.[9] A public refusal of this nature could signify a change in the environment of personal privacy. As companies, like Apple, present themselves as the proper entities to watch over our data,

---

1. John Perry Barlow, *Decrypting the Puzzle Palace*, 35 COMM. ACM 25, 26 (1992).

2. Senator Barack Obama, An Honest Government, a Hopeful Future, Address to the University of Nairobi (Aug. 28, 2006).

3. SPOKEO, http://www.spokeo.com (last visited July 30, 2017).

4. PEOPLELOOKUP, http://www.peoplelookup.com (last visited July 30, 2017).

5. PRIVATEEYE, http://www.privateeye.com (last visited July 30, 2017).

6. PUBLICRECORDSNOW, http://www.publicrecordsnow.com (last visited July 30, 2017). To be fair, there is no evidence that this website's name is actually representative of the company's response time.

7. *See* discussion *infra* Part II.

8. *See* discussion *infra* Part III.

9. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter [https://perma.cc/F2BA-5LLU].

however, consumers should consider whether they trust these companies, or the government for that matter, to safeguard their privacy.

The Pew Research Center released a report in 2015 that highlights the dramatic differences between how people feel about their personal data and how confident they are in either governmental agencies or corporations to keep that data safe.[10] The report details the findings of multiple surveys of adults in the United States, and was intended to ascertain their views of privacy and personal data following "the ongoing revelations of government surveillance activities introduced in 2013 by the ex-National Security Agency contractor Edward Snowden."[11] According to the study, 93% of Americans think it is important that they control who has their data,[12] while only 6% are "very confident" in the government's ability to keep that data secure.[13] Corporations didn't fare much better in the report, with credit card companies being trusted only slightly more than the government (9% "very confident"), and even less confidence was reported when dealing with telephone companies, email providers, and cable television providers (roughly 5% "very confident").[14]

If the American people have almost equally low confidence in corporations and governmental agencies, then perhaps both entities would benefit from taking actions that would generate greater confidence among the public. This Article examines the relevant threat that big data, and data brokers, in particular, pose to the privacy of individuals and what, if any, constitutional and legal rights affirmatively protect the privacy of personal information. There are four possible public- and private-sector solutions to challenge this threat: (1) more aggressive regulation under existing statutory authority; (2) expanding the authority of agencies to regulate through new legislation; (3) the possibility of a corporate right to privacy as a barrier to governmental intrusion; and (4) market-based solutions as small-scale strategies for individuals to protect their data. Each of these solutions has the potential to strengthen or add a layer of protection to the disclosure of private data, although none in isolation is fully sufficient. A more holistic approach—utilizing all of these solutions—can make personal information less accessible to undesired recipients, more secure and accurate for desired applications, and more

10. MARY MADDEN & LEE RAINIE, PEW RESEARCH CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE (2015).

11. *Id.* at 1.

12. *Id.* at 4.

13. *Id.* at 6.

14. *Id.* at 7.

transparent to the individual whose data it is, fundamentally, in the first place.

Part II of this Article examines the threat that the accumulation of information presents and the effect on personal privacy caused by the industry of data brokers that have proliferated around the use of big data. As individuals continue to disclose massive amounts of personally identifying information to companies around the globe, the collection and sale of this information has created a large and substantially unregulated industry that indiscriminately sells personal information about private citizens.

Part III looks at the interaction between the Constitution and the ever-evolving right to privacy, through the interpretation and decisions of the Supreme Court. The Part begins with a brief history of the right to privacy before moving on to the state of that right in modern society.

Part IV discusses current federal regulation of big data and the statutes, or lack thereof, that govern it. This Part features acts that affect the collection of emails, the reporting of health-related information and credit transactions, the criminalization of identity theft, and the transparency of government-held information.

Part V identifies and analyzes potential solutions, from both governmental and corporate entities to the burgeoning threat posed by big data. Solutions on the governmental side include more aggressive regulation and new legislation pertaining to the government's treatment of big data. As for the private sector, this Part examines the possibility of a corporate right to privacy as a possible tool to protect private rights, as well as market-based solutions that allow individuals to contract with companies to protect their personal data, although largely at a price.

Part VI briefly summarizes these facts, while suggesting that a multifaceted approach to combating big data would best counter the pervasive use of it. The proper "guardians of the galaxy of personal data" may be whoever can help protect it. More aggressive and expansive regulation could help the government rebound from public perception problems, given the relatively recent revelation that agencies were conducting widespread clandestine surveillance. A corporate right to privacy coupled with the emergence of privacy-protection firms could help add another layer of protection while simultaneously helping companies grow confidence with consumers. This composite approach would ensure that regardless of who our "guardians" are, our personal information and private data are better protected.

II. THE BIG DATA THREAT TO PERSONAL PRIVACY

The accumulation of personal information, and in particular the abuse of it by big data, poses a significant threat to the privacy of individual consumers. Due to technological advances in the collection, storage, and utilization of data, the sheer volume of information being aggregated today is unprecedented.[15] Information related to areas of particular sensitivity, like personal health care and credit reporting, is strictly monitored and regulated by law. For example, the Health Insurance Portability and Accountability Act of 1996 protects personal data that is associated with information regarding the personal health or care of that individual.[16] The Fair Credit Reporting Act (FCRA),[17] on the other hand, governs the use of consumer information by credit reporting agencies.[18] Most activities performed by data brokers and other companies that utilize big data, however, fall outside of the scope of the FCRA.[19] Because the FCRA does not regulate these activities and entities, no federal regulations are governing the collection of personal data by the largest of all information aggregators: data brokers.[20] The threat to consumers, unfortunately, which is increasingly apparent, does not stem solely from the collection of health- or credit-sensitive information. Aggregation of less-sensitive information still poses a distinct and potent threat to personal privacy, and the lack of regulation of these types of information is currently being exacerbated by the data broker industry and has only been minimally addressed by the government.

A. The Aggregation of Personal Information

The corporate desire for aggregated information is palpable, with an expanding online marketplace demanding increasingly accurate consumer information to target a diverse and unlimited mass of users.[21] America's ever-increasing dependence on the digital, rather than the physical, storage of information has resulted in an unprece-

---

15. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 4 (2014) [hereinafter BIG DATA OPPORTUNITIES].

16. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

17. 15 U.S.C. § 1681 (2012).

18. *Id.*

19. FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at i (2014) [hereinafter DATA BROKERS]. Data brokers and other companies using big data are exempt from the FCRA because they either do not qualify as a "consumer reporting agency" or the information they collect and sell does not qualify as a "consumer report" under the law. *Id.* at 5 n.10, 56 n.106; *see also* discussion *infra* Section IV.A.2.

20. *See* discussion *infra* Part V.

21. *See generally* BIG DATA OPPORTUNITIES, *supra* note 15.

dented accumulation of personal information.[22] According to the Supreme Court, "[t]he capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[23]

Social and professional interactions, in particular, are becoming reliant on third parties to foster both personal and business relationships as they are increasingly occurring online. Companies search for employees online, and potential employees research and apply for jobs online. Sites like LinkedIn provide networking opportunities, and professionals establishing an online business profile or resume is becoming commonplace and even expected.[24] Facebook sees its mission as keeping individuals from being uninformed of—or inadvertently excluded by—their social group,[25] and Twitter[26] has evolved to break news faster than any other news source.[27] Most people, however, are unaware of the gathering of information about them and the use and sale of that information for purposes such as future marketing and publishing.[28] And even when they are made aware of this price, many consumers continue to use these services, despite their expressed discomfort with the invasion of privacy, as they either rely on the service provided or are daunted by the scope of the problem and any solutions (or both).[29]

---

22. *See, e.g.*, IBM, 10 KEY MARKETING TRENDS FOR 2017 AND IDEAS FOR EXCEEDING CUSTOMER EXPECTATIONS 3 (2016) ("90% of the data in the world today has been created in the last two years alone . . . ."); *Big Data and the Future of Privacy*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/big-data [https://perma.cc/753S-5GY3] (finding that Google processes thousands of times more data in a day than exists in the entire printed material of the U.S. Library of Congress).

23. Sorrell v. IMS Health Inc., 564 U.S. 552, 579 (2011).

24. *About Us*, LINKEDIN, https://press.linkedin.com/about-linkedin [https://perma.cc/V974-EGEW] ("LinkedIn [is] the world's largest professional network with more than 546 million users in more than 200 countries and territories worldwide.").

25. Mark Zuckerberg, *Bringing the World Closer Together*, FACEBOOK (June 22, 2017, 10:25 AM), https://www.facebook.com/zuck/posts/10154944663901634 [https://perma.cc/KTV7-PANA]. Facebook changed its mission statement to "bring the world closer together," while the CEO's post announcing the change focused on Facebook gaining an even greater role in communities across the globe. *Id.*

26. TWITTER, https://twitter.com (last visited July 30, 2017).

27. *See* Barry Ritholtz, *How Twitter Is Becoming the First and Quickest Source of Investment News*, WASH. POST (Apr. 20, 2013), https://www.washingtonpost.com/business/how-twitter-is-becoming-your-first-source-of-investment-news/2013/04/19/19211044-a7b3-11e2-a8e2-5b98cb59187f_story.html [https://perma.cc/Q7RT-3YSM].

28. DATA BROKERS, *supra* note 19, at i.

29. *See* Thomas McMullan, *Guardian Readers on Privacy: 'We Trust Government Over Corporations'*, GUARDIAN (Oct. 18, 2015, 2:00 AM), http://www.theguardian.com/technology/2015/oct/18/guardian-readers-on-privacy-we-trust-government-over-corporations. *The Guardian* found that the public trusts the government more than private companies with their information, particularly as far as motivations for collecting personal data, but had rela-

1. "Big Data"

The Federal Trade Commission (FTC) notes that "[i]n today's economy, Big Data is big business."[30] But what is "big data," and why is it important? The term "big data" is somewhat undefined and varies depending on the industry, but generally the definition involves the collection of (1) large volumes of (2) complex, structured datasets that are (3) processed via some form of technology.[31] According to the Executive Office of the President, "definitions reflect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data."[32] Big data is viewed by some as property or even a public resource, presenting economic and other opportunities, while others see it as an expression of personal identity, threatening constitutional rights and personal liberties.[33] In determining whether the collection of information rises to the level of big data, experts may examine the data in terms of the "3 Vs."[34] The 3 Vs (volume, variety, and velocity) can be used to identify datasets that are "so large in volume, so diverse in variety or moving with such velocity, that traditional modes of data capture and analysis are insufficient."[35]

The first V, volume, describes the amount of information collected and utilized.[36] Declining costs in data processing and storage, coupled with an explosion of information provided by everything from websites to web-enabled devices,[37] have created large volumes of digital information for entities like corporations and governmental agencies

---

tively strong distrust of both public and private data collectors' ability to properly safeguard their privacy or use the data for permissible means. *Id.*

30. DATA BROKERS, *supra* note 19, at i.

31. JONATHAN STUART WARD & ADAM BARKER, UNDEFINED BY DATA: A SURVEY OF BIG DATA DEFINITIONS 1-2 (2013), https://arxiv.org/pdf/1309.5821.pdf [https://perma.cc/29XS-GRAG]. The authors concluded with the following definition: "Big data is a term describing the storage and analysis of large and or complex datasets using a series of techniques including, but not limited to: NoSQL, MapReduce and machine learning." *Id.* at 2. The computer-based processing is key to analyzing enormous, complex datasets. *Id.*

32. BIG DATA OPPORTUNITIES, *supra* note 15, at 2.

33. *Id.* at 3.

34. *See, e.g.*, *id.* at 4; FTC, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 1 (2016) [hereinafter DATA EXCLUSION].

35. BIG DATA OPPORTUNITIES, *supra* note 15, at 4.

36. *Id.*; *see also* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT—BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 2 (2014) [hereinafter TECHNOLOGICAL PERSPECTIVE].

37. *See* Lee Rainie & Janna Anderson, *The Internet of Things Connectivity Binge: What Are the Implications?*, PEW RESEARCH CTR. (June 6, 2017), http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications [https://perma.cc/S9WP-4NSY]. The "Internet of Things" describes the constellation of devices and appliances that are internet-connected and/or artificial-intelligence-enhanced, such as voice-activated assistants, smart electronics from thermostats to televisions, and monitoring devices to track one's health or secure one's home. *Id.*

to accumulate, explore, and potentially exploit. Another component that distinguishes big data is the wide variety of sources from which the information is usually obtained.

The second V, variety, encapsulates this idea, where personal information may be sourced from data which is either "born digital" or "born analog."[38] Information that is "born digital" is not derived from physical sources, but rather is created and exists entirely in digital form.[39] This data originates in a computer system and is created by users or the system itself, such as an email server, which records who sent a communication, to whom the message was sent, the time it was sent, and the content of the email.[40] In contrast, information that is "born analog" arises from the physical world, where behaviors and effects are captured by a sensor, such as a camera, a microphone, or an antenna.[41] This data is translated from its physical form into a digital format that can be analyzed together with information that was born digital.[42] Data that is born analog includes personal physical characteristics, forms filled out physically by individuals, and audio and video recordings of people and places, which is later converted to digital form or quantified to enable analysis and tabulation.[43]

The final V, velocity, encompasses types of data that are created and sent very quickly, increasingly offering analysis in real time, with the ability to affect a person's immediate environment and decisionmaking.[44] Global Positioning System (GPS) data, click-stream tracking on websites, and automatically associated time or location information are all examples of high-velocity interactions that expose information about individuals using those services.[45]

Big data is not inherently bad, or innately good for that matter: it can be used or misused for both positive and negative ends, for a variety of purposes, and by a wide variety of actors. Big data is used to obtain insights into individual behavior, preferences, and patterns—

---

38. *See* TECHNOLOGICAL PERSPECTIVE, *supra* note 36, at 19, 22.

39. *Id.* at 19-21.

40. *See id.* Other types of "born digital" information include data such as cellphone metadata, GPS location data, credit card swipes, RFID tags, and keystrokes and clicks from computers, tablets, phones, and video games. *Id.* at 19-20.

41. See *id.* at 22-23.

42. *Id.*

43. *See id.* Other types of "born analog" information include data such as voice and video content of phone calls, surveillance videos, medical imaging and data from personal health trackers, and fingerprint and DNA data. *Id.* at 22.

44. BIG DATA OPPORTUNITIES, *supra* note 15, at 5. Indeed, there is high demand to provide analysis or responsive transmission of certain types of data in ways that benefit users instantly, such as the need for mobile mapping applications to have immediate, accurate access to the user's location. *Id.*

45. *See id.*

enabling personalization, learning, and even prediction.[46] Governmental agencies and corporations alike have made efforts to take advantage of big data to "boost economic productivity, drive improved consumer and government services, thwart terrorists, and save lives,"[47] by making processes more efficient, accurate, and effective. On the governmental side, for example, the Centers for Medicare and Medicaid Services use big data to identify likely instances of fraud, while the Defense Advanced Research Projects Agency (DARPA) uses big data to help military personnel deployed in the field assess and solve operational challenges.[48] On the private sector side, big data has been used in the neonatal intensive care unit (NICU) to identify newborns who are at greater risk of illness.[49] Additionally, big data has played a substantial role in targeted or retargeted advertising,[50] where companies use data analytics to advertise to specific consumers that already have a strong preference for their product.[51] In fact, one emerging corporate marketing technique, called customer relationship marketing (CRM) retargeting (or data onboarding), combines online and offline data to target and deliver advertising to online users based on their identity.[52]

A 2016 White House report recognized that big data analytics are often assumed to be unbiased and objective, disinterestedly revealing the true behavior and characteristics of consumers through large-scale inputs and data-driven algorithms.[53] The report focused on the impact of big data on access to opportunities and examined the permeating influence of big data on the activities and lives of modern

46. *Id.* at 5-7.

47. *Id.* at 5.

48. *Id.* at 6.

49. *Id.*

50. Christian Madsbjerg & Mikkel B. Rasmussen, *Advertising's Big Data Dilemma*, HARV. BUS. REV. (Aug. 7, 2013), https://hbr.org/2013/08/advertisings-big-data-dilemma [https://perma.cc/2KL4-BPVT].

51. Ganesh Iyer, David Soberman & J. Miguel Villas-Boas, *The Targeting of Advertising*, 24 MARKETING SCI. 461, 461 (2005) (discussing how companies that are able to use targeted advertising target the segment of consumers who show a strong preference for their product rather than comparison shoppers).

52. *See* Daniel Newman, *CRM Targeting? The Next Wave of Big Data Utilization for Marketing*, FORBES (June 3, 2015, 9:26 PM), http://www.forbes.com/sites/danielnewman/2015/06/03/crm-retargeting-the-next-wave-of-big-data-utilization-for-marketing (noting that CRM retargeting is leading advertisers to target online users based "more on identity than on behavior or preference"); *see also* DATA BROKERS, *supra* note 19, at v. Data onboarding involves placing a cookie on a user's computer with information about that user's identity or preferences attached. *Id.* at 27. Often, advertisers first define "segments" of consumers, based on their characteristics or shopping habits, and attach that segment identity to the cookie as well. *Id.* at 27-28.

53. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS 6 (2016) [hereinafter BIG DATA ALGORITHMS].

Americans, including access to credit, employment, higher education, and criminal justice.[54] The case studies in this report revealed the potential for discrimination and prejudice based on either the inputs used in the analytics or issues with the design and functioning of the algorithm itself.[55] As industry experts have expressed, big data can expand customer intelligence or the ability of a company to understand its customers; improve operational efficiencies through predictive analytics; create new business processes based on mobile technologies; and offer marketing solutions to companies that are ill-equipped to build robust datasets.[56] Undoubtedly, big data provides and potentially foreshadows significant benefits to governmental agencies, corporations, and consumers. However, to take advantage of big data, private and public entities must first have accurate, efficient access to it—which is precisely where data brokers come into play.

2. Data Brokers: The Quintessential Personal Data Aggregators

Companies that amass, aggregate, and resell personal information are known as "data brokers."[57] Data brokers develop files on individual consumers, most likely including you,[58] based on both online and offline data, containing everything from state records and census reports to in-store purchases and personal internet browsing history.[59] According to the FTC, most consumers are unaware that data brokers even exist and to what extent they are tracking our individual activities.[60] Data brokers, like Acxiom—one of the world's largest consumer information companies[61]—claim that they "don't want to know intimate facts about you,"[62] but that is exactly what they are selling.

---

54. *Id.* at 10.

55. *Id.* at 6-11.

56. Sashi Reddi, *4 Ways Big Data Will Transform Business*, CSC WORLD, Winter 2013, at 12-13, https://web.archive.org/web/20140211063333/https://assets1.csc.com/cscworld/downloads/CSCWorld_Winter_2013.pdf [https://perma.cc/UG62-LQ7Z].

57. DATA BROKERS, *supra* note 19, at 3.

58. *See id.* at iv (noting that the FTC found that one data broker alone had "3000 data segments for nearly every U.S. consumer").

59. *Id.* at iv-v.

60. *Id.* at 3.

61. *See* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html ("[A]nalysts say [Acxiom] has amassed the world's largest commercial database on consumers . . . ."); *see also* ACXIOM, http://www.acxiom.com (last visited July 30, 2017).

62. Acxiom, *How Do Companies Get Data About Me and What Do They Do with It?*, ABOUTTHEDATA.COM, https://www.aboutthedata.com/how [https://perma.cc/2WH8-25RD]. Although Acxiom promises that they do not want or share "intimate" facts about you, they limit the definition of intimate to include things such as social security numbers, credit and

Data brokers primarily deal in the sale of datasets, analytical tools, risk mitigation techniques, and people search products.[63] Data brokers may sell particular data points, like an individual's email address, to outside companies, enabling them to advertise directly to the consumer.[64] They may also sell analytical tools to sift through consumer datasets in order to better target potential customers.[65] Beyond supplementing marketing strategies, data brokers often sell risk mitigation products that are used to detect and prevent fraud by, for example, confirming someone's identity or flagging suspicious behavior.[66] Finally, many data brokers use their access to a "galaxy" of consumer information to create or supply the data for "people search" websites.[67] These sites allow users to find detailed information on individuals regardless of their association with those people or the purpose of such a search.[68] As is the case with much of the discussion concerning the flow of personal data, access to information provided by data brokers carries both positive and negative potential effects. On the one hand, among other potential benefits, people search services can unite old friends, provide invaluable background information on potential employees, and inform companies about their customers.[69] On the other hand, these services have been used to facilitate criminal acts—such as tax fraud[70] and stalking[71]—as well as legal, but unsettling or improper acts, such as predatory targeting of victims of rape, individuals who have AIDS, or seniors with dementia.[72]

"detailed" financial information, and medical information. *Id.* Not everyone would agree that those are the only intimate facts about a person.

63. DATA BROKERS, *supra* note 19, at ii-iii.

64. *Id.* at ii.

65. *Id.* For example, data brokers might analyze a company's customer data to determine what region and media to target or to rank customers based on their web presence or potential response to marketing. *Id.* at ii-iii.

66. *Id.* at iii.

67. *Id.*

68. *Id.*

69. *Id.*

70. Francisco Alvarado, *Miami Drug Dealers Used People Search Website for Tax Return Fraud Scheme*, FLA. CTR. FOR INVESTIGATIVE REPORTING (Aug. 21, 2015), http://fcir.org/2015/08/21/miami-drug-dealers-used-people-search-website-for-tax-return-fraud-scheme [https://perma.cc/YX23-FP4T] (discussing a scheme in which two drug dealers in Miami, Florida used a people search website to steal the personal information of unassociated individuals in order to obtain fraudulent tax refunds).

71. DATA BROKERS, *supra* note 19, at 48.

72. Melanie Hicken, *Data Brokers Selling Lists of Rape Victims, AIDS Patients*, CNN (Dec. 19, 2013, 12:38 PM), http://money.cnn.com/2013/12/18/pf/data-broker-lists [https://perma.cc/5JJQ-R644] (noting that, for example, a list of seniors with dementia could be used to market predatory financial offers).

B. The Dangers of Big Data

While big data, and the data brokers that help assemble and disperse large datasets, can certainly be helpful or even valuable, the accumulation of personal and identifying information poses a substantial and very real risk to consumers. The potential for harm is rooted in both how the collected information is used and how that information can be stolen or exposed due to a security breach.[73] Additionally, for most existing big datasets, there is no meaningful way for consumers to determine who has their information, how to access or correct it, or how to limit the sharing of information if that is even possible.[74] Each type of potential harm is distinct, dangerous, and has in fact resulted in serious consequences for consumers through, for example, lost opportunities due to biases or inaccuracies in the data or algorithms.[75] These harms, on their own and in aggregate, present a significant threat to personal privacy that requires serious and immediate attention.

1. The Misuse of Data in General

The potential for consumer harm from the misuse of big data is evident in both corporate and governmental environments. As the White House report on big data's impact on opportunities noted, sharing information with companies "enables a greater degree of improvement and customization, but this sharing also creates opportunities for additional uses of our data that may be unexpected, invasive, or discriminatory."[76] Misuse by individuals and entities can range from broad, sweeping actions to small, specific instances of conduct. Regardless of the scope and effect of such misuse, though, the temptation to invade the personal privacy of others in the context of the proliferation of big data can result in real harm to consumers.

This harm may include invasions of privacy that are improper or disquieting, but legally permissible. The now-infamous PRISM program is one example of big data collection and use by a governmental agency that was wide-ranging in effect and extremely controversial in terms of public perception. PRISM was a surveillance system used by the National Security Agency (NSA) to obtain information regard-

73. DATA BROKERS, *supra* note 19, at v-vi.

74. *Id.* at 50 (outlining recommendations for new legislation to provide consumers with access to their data and an ability to "opt-out" of having one's data shared for marketing purposes).

75. BIG DATA ALGORITHMS, *supra* note 53, at 6-8.

76. *Id.* at 5.

ing foreign intelligence[77] and operated in secrecy until NSA contractor-turned-whistleblower Edward Snowden exposed the program's existence.[78] The program was authorized by section 702 of the Foreign Intelligence Surveillance Act (FISA),[79] and allows the government, with FISA Court approval, to obtain and collect information, such as emails, photos, and phone logs, from electronic communication service providers.[80] As the Director of National Intelligence emphasized at the time that the public learned of the program, "PRISM is *not* an undisclosed collection or data mining program. It is an internal government computer system used to facilitate the government's *statutorily authorized collection* . . . from electronic communication service providers."[81] While the exposure of PRISM was met with public attention and even outrage,[82] clandestine operations performed by the government are only one broad way in which big data presents harms that are difficult to identify and prevent, yet intuitively feel to be violations of our collective privacy rights.

2. Relying on Inaccurate Information

Incorrect information, or accurate information that is incorrectly interpreted, can also present unwanted consequences for consumers.[83] Individuals may be erroneously excluded from certain transactions, such as loans or large purchases, based on incorrect information,[84] though data brokers are quick to point out that the exchange of information about the customer is intended to "inform a transaction, not stop it."[85] Big data may reinforce prejudices and finan-

---

77. DIR. OF NAT'L INTELLIGENCE, FACTS ON THE COLLECTION OF INTELLIGENCE PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 1 (2013) [hereinafter PRISM].

78. *See* Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST: WONKBLOG (June 12, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date [https://perma.cc/PT24-DELQ].

79. 50 U.S.C. § 1881a (2012).

80. PRISM, *supra* note 77, at 171.

81. *Id.* (emphasis added).

82. *See, e.g.*, *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC (Jan. 7, 2014), http://www.bbc.com/news/world-us-canada-23123964 [https://perma.cc/CMH3-KV6P]; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/K74T-SJVS]; Steven Levy, *How the NSA Almost Killed the Internet*, WIRED (Jan. 7, 2014, 6:30 AM), https://www.wired.com/2014/01/how-the-us-almost-killed-the-internet [http://perma.cc/5FAN-RD3U].

83. DATA BROKERS, *supra* note 19, at v.

84. *Id.* Companies, such as insurers, also often rely on big data to determine rates and service levels. *Id.* at 48.

85. Sam Pfeifle, *Industry Reaction to FTC Data Brokers Report: Eh.*, IAPP (May 28, 2014) (quoting Stuart Pratt, president and CEO of the Consumer Data Industry Associa-

cial disparities as well. According to the FTC, "when big data is used to target ads, particularly for financial products, low-income consumers who may otherwise be eligible for better offers may never receive them."[86] Similarly, online companies that utilize big data may charge more depending on the location of the user, which can result in higher-priced goods and services for lower-income or minority communities.[87]

3. Accurate but Revealing Information

Another potential threat to consumers, and one that inescapably challenges the boundaries of the constitutional right to privacy, is the danger that big data poses when it *is* accurate. Companies may create and employ specific datasets for particular marketing purposes, but by collecting, organizing, and combining that information, the company may inadvertently expose sensitive or embarrassing information about the consumer to third parties.[88] In this instance, the more accurate and robust the information, the greater the potential for harm. One study found that researchers could predict defining characteristics about users, such as a user's sexual orientation or political affiliation, based on Facebook "Likes" combined with limited survey data.[89] Considering this predictive ability, and the pervasiveness with which companies utilize big data, it is easy to imagine a scenario where a company sends marketing materials to a prospective customer that exposes private information about him or her. For example, if the marketing is based on data that indicates a consumer's sexual preference for the same sex, the materials could reveal the individual's private, and perhaps unknown, sexual orientation to anyone that may come upon the mail.

Predictive analytics based on big data may also deny customers opportunities through no fault of their own.[90] The accuracy of predictive analysis depends first on the quality of the information on which it is based,[91] but even where the data is accurate, companies may

---

tion), https://iapp.org/news/a/industry-reaction-to-ftc-data-brokers-report-eh [https://perma.cc/8M9Z-XDCK].

86. DATA EXCLUSION, *supra* note 34, at 10.

87. *Id.* at 11.

88. *Id.* at 10.

89. Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802, 5803-04 (2013) ("The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases.").

90. DATA EXCLUSION, *supra* note 34, at 9.

91. *See* Benjamin T. Hazen et al., *Data Quality for Data Science, Predictive Analytics, and Big Data in the Supply Chain Management: An Introduction to the Problem and Suggestions for Research and Applications*, 154 INT'L J. PROD. ECON. 72, 72-80 (2014).

draw unwarranted conclusions or associations. In particular, credit card companies have used big data tools to rank customers,[92] and, in some cases, companies have even lowered a customer's credit limit based on similarities between that customer's shopping habits and the habits of other customers with poor repayment histories.[93] Unfair or unjust decisionmaking techniques like these show how companies may be tempted to abuse access to customer information and how overconfidence in big data may lead to erroneous judgments or even civil liability.[94]

4. Reidentifying Anonymous Data

As big data has evolved, one fundamental aspect of the technology—the ability to combine datasets and gain insight through analyzing the aggregated data[95]—has matured to the point that an individual's information found in anonymous datasets may now be reidentified, or deanonymized, by combing the information with other inputs.[96] This process of combining multiple anonymous datasets in order to obtain personally identifying information is known as the "mosaic effect."[97] Technologies that are able to reassemble identifying personal data strip big data of one of the few safeguards employed and touted by the industry; namely, the anonymization of information.[98] While problems related to the ineffective anonymity of datasets have been known for years,[99] technological improvements and the increased availability of information have compounded the problem.[100] Somewhat disturbingly, for example, a 2013 study was able to correctly identify up to ninety-seven percent of publicly available profiles in the Personal Genome Project by matching demographic information found in the profiles to public records.[101]

92. DATA EXCLUSION, *supra* note 34, at 9 (noting that scores were used to reduce consumers' credit lines based on their purchase history).

93. *Id.*

94. *See* Press Release, FTC, Subprime Credit Card Marketer to Provide At Least $114 Million in Consumer Redress to Settle FTC Charges of Deceptive Conduct (Dec. 19, 2008), https://www.ftc.gov/news-events/press-releases/2008/12/subprime-credit-card-marketer-provide-least-114-million-consumer [https://perma.cc/7H6B-SJBF].

95. DATA EXCLUSION, *supra* note 34, at 1.

96. BIG DATA OPPORTUNITIES, *supra* note 15, at 8.

97. *Id.*

98. *Id.*

99. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

100. *See generally* BIG DATA OPPORTUNITIES, *supra* note 15.

101. LATANYA SWEENEY ET AL., IDENTIFYING PARTICIPANTS IN THE PERSONAL GENOME PROJECT BY NAME, HARV. WHITE PAPER 1021-31 (2013), http://dataprivacylab.org/projects/pgp/1021-1.pdf [https://perma.cc/6L5G-JRP2].

III. BIG DATA AND THE CONSTITUTION

Privacy, or the state of being alone or away from others,[102] remains highly valued by the vast majority of Americans.[103] Although not specifically enumerated in the U.S. Constitution,[104] the Supreme Court has recognized privacy as a fundamental right guaranteed by the Constitution since the 1960s,[105] and legal protections for privacy date back much further.[106] The Framers of the Constitution grounded many of the early amendments, primarily in the Bill of Rights, in privacy protections. The First, Third, Fourth, and Fifth Amendments, for instance, all involve aspects of privacy and protection from having that privacy invaded by the government. The First Amendment guards the sanctity of individual thought and the privacy of beliefs by proscribing the government from enacting laws limiting the free exercise of religion, speech, and assembly.[107] The Third Amendment guards the privacy of one's home by barring the compulsory quartering of soldiers.[108] The Fourth Amendment guards the privacy of one's person and belongings by protecting against unreasonable search and seizure.[109] The Fifth Amendment guards the privacy of thought and self-determination by protecting against self-incrimination and requiring due process of law.[110] Finally, the Ninth Amendment provides the basis for finding certain rights outside of the language of the Constitution: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[111] These Amendments, considered together, permitted the Supreme Court to codify the right to privacy as one of our fundamental constitutional guarantees.[112]

---

102. *Privacy*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/privacy [https://perma.cc/Y936-HU6D] (last updated Feb. 24, 2018).

103. MADDEN & RAINIE, *supra* note 10, at 4 (noting that 88% of participants in the study reported that it was important not to "have someone watch or listen to them without their permission" and, concerning personal information, 90% expressed the importance of controlling what information about them was collected, while 93% said it was important to control who could obtain their data).

104. *See generally* William M. Beaney, *The Right to Privacy and American Law*, 31 LAW & CONTEMP. PROBS. 253 (1966).

105. *See* Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965); Poe v. Ullman, 367 U.S. 497, 523-55 (1961) (Harlan, J., dissenting).

106. *See* 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 168 (1769) (containing information relating to the crime of eavesdropping).

107. U.S. CONST. amend. I.

108. *Id.* amend. III.

109. *Id.* amend. IV.

110. *Id.* amend. V.

111. *Id.* amend. IX.

112. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

A. A Brief History of the Right to Privacy

The Supreme Court's recognition of privacy as a guaranteed right began in the 1920s. The initial groundwork was set forth in 1923, in *Meyer v. Nebraska*.[113] The Court held that a Nebraska law prohibiting any subject to be taught in a foreign language was unconstitutional, relying on protections not explicit in the Constitution to form its decision based largely on the concept of "liberty."[114] Justice McReynolds, who delivered the opinion, wrote:

> While this court has not attempted to define with exactness the liberty thus guaranteed, the term has received much consideration and some of the included things have been definitely stated. Without doubt, it denotes not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men.[115]

This broad definition of liberty, which was echoed by the Supreme Court two years later in *Pierce v. Society of Sisters*,[116] was the foundation on which the Court based its reading of constitutional privacy rights in the 1960s. In determining whether an individual's privacy rights have been violated, the Supreme Court recognizes that "certain interests require particularly careful scrutiny of the state needs asserted to justify their abridgment."[117] Therefore, governmental actions that affect individual privacy, as a component of liberty, require states to show a credible and convincing justification for the intrusion because reviewing courts examine the actions under strict scrutiny, the most demanding standard of judicial review.[118]

---

113. 262 U.S. 390 (1923).

114. *Id.* at 399. The Court extrapolated from the prohibition in the Fourteenth Amendment of any state depriving "any person of life, liberty, or property, without due process of law." *Id.* (quoting U.S. CONST. amend. XIV).

115. *Id.*

116. 268 U.S. 510, 534-35 (1925) (holding that the Nebraska law interfered with the liberty of parents to choose how to raise their children).

117. Poe v. Ullman, 367 U.S. 497, 543 (1961) (Harlan, J., dissenting); *see also Griswold*, 381 U.S. at 486-99 (Goldberg, J., concurring) (describing the right to privacy, in marital relations at least, as "fundamental and basic").

118. Skinner v. Oklahoma, 316 U.S. 535, 541 (1942) (holding that strict scrutiny is required for review of state laws that irreversibly deprive persons of a basic liberty, such as procreation). Generally, strict scrutiny requires the state to show that the challenged law is narrowly drawn to further a compelling state interest, using the least restrictive means to further that interest. *See, e.g.*, Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 871 (1992); Roe v. Wade, 410 U.S. 113, 155 (1973).

1. Recognition of Privacy Rights

The seminal privacy case, *Griswold v. Connecticut*,[119] represents the first instance where the Supreme Court categorically confirmed the right of privacy for individuals.[120] The Court came to this conclusion based, in part, on a dissenting opinion from four years earlier in 1961.[121] In *Poe v. Ullman*,[122] Justice Douglas wrote an impassioned dissent,[123] urging that the Court recognize privacy considerations in deciding the case: "This notion of privacy is not drawn from the blue. It emanates from the totality of the constitutional scheme under which we live."[124] Building on this concept, the Court in *Griswold* found that zones of privacy were created by constitutional guarantees.[125] Citing the Third, Fourth, Fifth, and Ninth Amendments, in addition to stare decisis,[126] the Court identified a right of privacy that it considered "older than the Bill of Rights."[127] Justice Douglas, this time writing on behalf of the majority, was able to reassert his once-rebuffed view on privacy, proclaiming that "the right of privacy which presses for recognition here is a legitimate one."[128]

Privacy protection continued to play a crucial role in decisions following Justice Douglas's 1965 dissent in *Griswold*. For example, in 1967, the Supreme Court set the basic rule that warrantless searches are per se unreasonable, with a few exceptions, under the Fourth Amendment in *Katz v. United States*.[129] The Court in *Katz* focused on a person's expectation of privacy,[130] a principle which would continue to play a role in future Supreme Court decisions.[131] The unanimous 1969 Supreme Court decision in *Stanley v. Georgia*[132] held that the

119. 381 U.S. 479 (1965).

120. *Id.* at 484. *See generally* Beaney, *supra* note 104.

121. *See Griswold*, 381 U.S. at 484.

122. 367 U.S. 497 (1961).

123. *Id.* at 509-522 (Douglas, J., dissenting).

124. *Id.* at 521 (citations omitted).

125. *Griswold*, 381 U.S. at 484.

126. *Id.* at 484-85.

127. *Id.* at 486.

128. *Id.* at 485.

129. 389 U.S. 347, 357 (1967).

130. *Id.* at 359. The *Katz* Court held the electronic surveillance of a telephone booth was a search, and therefore, a violation of the Fourth Amendment. *Id.* at 357-58. Justice Harlan's concurring opinion summarized the decision as holding that a phone booth is a type of place, like the home, where a person has an objectively reasonable expectation of privacy and that electronic, as well as physical, intrusion into those spaces is presumptively invalid in the absence of a warrant. *Id.* at 360-61 (Harlan, J., concurring).

131. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

132. 394 U.S. 557 (1969).

personal possession of obscene material, taken by itself, was protected under the Fourth and Fourteenth Amendments.[133] The Court stressed that regulating obscenity was indeed a power held by states, but concluded that the Constitution limited such power in order to protect private citizens' liberty.[134] The Court noted that "[f]or also fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."[135]

The following decade also saw important cases relying on protections derived from the right to privacy.[136] In the momentous 1973 case, *Roe v. Wade*,[137] for instance, the Supreme Court determined that the right to privacy protected a woman's personal choice to proceed with, or terminate, a pregnancy.[138] In holding that the near-universal ban on abortions challenged in Texas criminal abortion statutes was unconstitutional,[139] Justice Blackmun noted that "the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."[140] The Supreme Court also often contemplated well-established customs and traditions to help inform decisions on personal privacy. For example, in *Kelley v. Johnson*,[141] the Court looked at the prevalence among states and local communities of imposing constraints on the personal appearance of uniformed law enforcement officers to determine the permissibility of those constraints.[142] Finding that the vast majority of states employed restrictions on uniformed police personnel—such as the mandatory haircuts at issue in the case—and that such techniques were used to meet the public need to more easily identify officers and to unify the police force, the Court found no violation of the liberties guaranteed by the Constitution.[143] Similarly, in *Moore v. East Cleveland*,[144] the Supreme Court relied on well-established American traditions related to the privacy and sanctity of

133. *Id.* at 568.

134. *Id.* The Court emphasized the right to receive information and ideas, regardless of their perceived "social worth," and the fundamental right to read and observe whatever a person wants in the privacy of their own home, as components of the bedrock unconstitutionality of the government trying to control what its citizenry thinks and believes. *Id.* at 564-65.

135. *Id.* at 564.

136. *See, e.g.*, Kelley v. Johnson, 425 U.S. 238 (1976); Roe v. Wade, 410 U.S. 113 (1973).

137. *Roe*, 410 U.S. 113.

138. *Id.* at 164.

139. *Id.* at 166.

140. *Id.* at 152.

141. *Kelley*, 425 U.S. 238.

142. *Id.* at 248.

143. *Id.* at 248-49.

144. 431 U.S. 494 (1977).

family in holding that the choice of living arrangements within a family, as a liberty interest, was protected under the Constitution.[145]

2. Limiting Protection Due to the Expectation of Privacy

The contours of privacy protection, however, began to become more defined and narrow by the end of the 1970s and into the 1980s, with the Supreme Court focusing on the reasonableness of an individual's expectation of privacy in a given situation as a means to determine whether an intrusion on his privacy was reasonable. In 1978, the Supreme Court, in *Zurcher v. Stanford Daily*,[146] declined to extend privacy protections under the Fourth Amendment to warranted searches of third-party premises, even of newspaper offices.[147] In 1979, the Court, in *Smith v. Maryland*,[148] failed to apply privacy rights to records of telephone numbers dialed.[149] Both of these cases examined the expectation of privacy held by the individual. Likewise, Supreme Court decisions throughout the 1980s analyzed potential invasions of individual privacy and whether an expectation to that privacy existed to begin with.[150] The decision in *California v. Greenwood*,[151] for example, eliminated privacy rights to personal items discarded as garbage and left on a public street.[152] The Court decided that by placing the trash on the curb, the respondents had sufficiently surrendered and exposed their items to the public for the express purpose of giving those items up to a third party, negating any reasonable expectation to privacy.[153]

3. Cultural Values and the Right to Privacy

More recent privacy-related cases share a common theme with older cases. The decisions in these cases mirror broader cultural changes occurring in America at the time and represent an integration of those cultural shifts into the modern concept of privacy. In *Roe*

145. *Id.* at 500-01, 504 (extending constitutional protections for family relationships and childrearing to non-nuclear family relations, such as grandparents, aunts, and uncles).

146. 436 U.S. 547 (1978).

147. *Id.* at 567-68.

148. 442 U.S. 735 (1979).

149. *Id.* at 745-46 (holding that a person does not have a legitimate or actual expectation of privacy in the phone numbers he or she dials).

150. *See, e.g.*, Florida v. Riley, 488 U.S. 445 (1989); California v. Greenwood, 486 U.S. 35 (1988).

151. 486 U.S. 35 (1988).

152. *Id.* at 37, 40.

153. *Id.* at 40-41. The Court emphasized that outdoor garbage disposal is intended to be picked up by garbage collectors and could also be searched by animals, children, scavengers, and strangers. *Id.*

v. Wade, for example, privacy considerations encompassing a woman's decision whether to continue her pregnancy, in the context of progress in women's rights, led to the Court's invalidation of abortion statutes.[154] *Cruzan v. Missouri Department of Health*,[155] a Supreme Court decision from 1990, and *Lawrence v. Texas*,[156] decided in 2003, also involved privacy-related challenges that reflected changes in social beliefs. The *Cruzan* Court dealt with the difficult decision of two parents to possibly terminate the life-prolonging treatment of their daughter, who was in a permanent vegetative state.[157] The Court found that there was a protected liberty interest in the private determination to refuse medical treatment.[158]

Thirteen years later, the Supreme Court addressed privacy concerns surrounding homosexuality in *Lawrence v. Texas*. The Court held a Texas statute that made particular private sexual acts illegal, and which was used to prosecute homosexual males, was unconstitutional.[159] These cases show that Supreme Court privacy considerations are broadened or narrowed in response to changes in society and American culture as a whole, whether those changes are due to advances in women's rights, complications due to advancements in medical care and technology, or wider societal acceptance of same-sex relationships.[160] The most consequential cultural change reflected in modern privacy rights is, of course, tied to the invention and proliferation of personal computers and the internet, and the explosion of digital data, information, and websites created through the linkage of each.

B. Modern Privacy Rights and Personal Data

The rapid introduction of new technologies and the conversion of physically recorded information into digital data has resulted in unforeseen privacy concerns being brought before the Supreme Court. The ease with which information, particularly private data from personal devices, can be recorded and accessed today can result in information recovered from criminal suspects, yet not admissible in court. The "exclusionary rule," which bars prosecutors from submitting illegally obtained evidence in court, is a judicial doctrine used to deter Fourth Amendment violations.[161] Under the exclusionary rule,

154. Roe v. Wade, 410 U.S. 113, 166 (1973).
155. 497 U.S. 261 (1990).
156. 539 U.S. 558 (2003).
157. *Cruzan*, 497 U.S. at 266.
158. *Id.* at 278.
159. *Lawrence*, 539 U.S. at 578-79.
160. *See* Obergefell v. Hodges, 135 S. Ct. 2584, 2598-99 (2015).
161. *See, e.g.*, Davis v. United States, 564 U.S. 229, 236-37 (2011).

any evidence derived from an improper, warrantless invasion of an individual's Fourth Amendment rights cannot be admitted into evidence at trial against them.[162] Warrantless searches of a suspect that take place during an arrest, however, are not subject to the exclusionary rule, so long as the search is lawful and limited to the arrestee's person and the surrounding area "within his immediate control."[163] According to the Supreme Court, warrantless searches are permissible outside of the arrestee's person only to cover "the area from within which he might gain possession of a weapon or destructible evidence."[164] The Court emphasizes the twin risks of potential harm to an officer and the opportunity for destruction of evidence as the foundational justifications for why such a search may not violate an individual's constitutional rights.[165] These principal risks become problematic, however, when assessing evidence and personal information that is digital, not physical in nature.

1. Addressing the Evolving Nature of the Right to Privacy

In an environment where judges and courts often struggle to keep up with rapidly developing technologies, it can be difficult to determine when a warrantless search is subject to the exclusionary rule because of shifts in the Supreme Court's position that affect the admissibility of evidence in a pending case. The 2011 case, *Davis v. United States*,[166] involved a warrantless search that was compliant with then-existing Supreme Court precedent when the search was conducted.[167] Under the 1981 precedent of *New York v. Belton*,[168] the passenger compartment of a vehicle was a permissible place for a police officer to search when making a lawful custodial arrest of vehicle passengers.[169] However, in 2009, the Court decided *Arizona v. Gant*,[170] in which the Court declined a broad reading of *Belton*.[171] Instead, the Court created a two-part rule that determined whether the search of a vehicle was unreasonable, and thus unconstitutional, based on whether the arrestee could reach items in the search area and whether the police had reason to believe that there was evidence in the searched area related to

162. *Id.* at 231-32.
163. Chimel v. California, 395 U.S. 752, 763 (1969).
164. *Id.*
165. *Id.*
166. *Davis*, 564 U.S. 229.
167. *Id.* at 235.
168. 453 U.S. 454 (1981).
169. *Id.* at 462-63.
170. 556 U.S. 332 (2009).
171. *Id.* at 348.

the crime for which the individual was being arrested.[172] Due to the timing of the appeal process in *Davis*, the warrantless search in question was lawful under *Belton* when it was conducted, yet unlawful at the time of appeal due to the newly defined rule in *Gant*.[173] The *Davis* Court decided that when the police conduct a search which is reasonable and therefore legal at the time of the search, under governing case law, the exclusionary rule does not apply.[174] As technology and jurisprudence continue to evolve and courts respond via individual judicial decisions, modern privacy protections will likely develop in relation to technological evolution.

2. Modern Technology and Privacy Protection

In 2014, the Supreme Court addressed privacy issues surrounding one of the most ubiquitous pieces of technology in modern society, the cell phone. In *Riley v. California*,[175] the Court was presented with the consolidation of two separate appellate cases, both involving evidence that had been obtained from the defendant's cell phone through a warrantless search.[176] In order to determine whether to allow a particular type of warrantless search, the Court generally weighs the degree of intrusion on the individual's privacy against how necessary the search is to further a legitimate governmental interest.[177]

In recognition of the fundamental difference between physical objects and digital data, the Court declined to extend the categorical rule found in *United States v. Robinson*,[178] a pre-cell phone case from 1973 where the Supreme Court held that the warrantless search of a suspect arrested in the course of a traffic stop was a permissible intrusion under the Fourth Amendment.[179] The *Robinson* Court acknowledged that the lawful intrusion of personal rights incident to arrest did not alone permit any additional intrusion on the suspect's personal privacy,[180] following the precedent set four years earlier by *Chimel v. California*.[181] The Court did, however, find another justification for such a warrantless search: "The justification or reason for the authority to search incident to a lawful arrest rests quite as much on the need to

172. *Id.* at 343.
173. Davis v. United States, 564 U.S. 229, 235-36 (2011).
174. *Id.* at 249-50.
175. 134 S. Ct. 2473 (2014).
176. *Id.* at 2480.
177. *Id.* at 2484 (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
178. 414 U.S. 218 (1973).
179. *Id.* at 235-36.
180. *Id.* at 225-26.
181. 395 U.S. 752 (1969).

disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial."[182]

The Supreme Court in *Riley* distinguished *Robinson* by noting that the risks presented by physical objects during an arrest were absent when dealing with cell phone searches; in other words, cell-phone data could not threaten the arresting officer or risk the destruction of potential evidence in the same way that physical items could.[183] Justice Roberts, writing the opinion for the Court, noted that unlike physical searches, cellphone searches "place vast quantities of personal information literally in the hands of individuals."[184] Following the Supreme Court's tradition of defining privacy rights within the context of social norms, *Riley* represents the Court's recognition that a cell phone represents a distinct class of item, different and far more valued than other personal items.[185] People have evolved to literally love their cell phones,[186] which makes this type of privacy protection crucial to the protection of personal privacy, as delineated by future cases.[187]

3. Constitutional Protection for Personal Data

As for personal data, the Constitution, as currently interpreted, does little to protect consumers from the aggregation of information that they have disclosed to corporate actors. The third-party doctrine, as seen in cases like *United States v. Miller*[188] and *Smith v. Maryland*,[189] insulates companies that accumulate and combine information.[190] In *Miller*, the U.S. Bureau of Alcohol, Tobacco, and Firearms (ATF) obtained evidence through subpoenas issued to the defendant's banks.[191] Without notice to or approval from their client (Miller), the banks turned over the desired bank records to the gov-

182. *Robinson*, 414 U.S. at 234.

183. Riley v. California, 134 S. Ct. 2473, 2484-85 (2014).

184. *Id.* at 2485.

185. *See id.* at 2488-91 (discussing the many ways that cell phones are different from other items someone carries in their pockets, other types of records, and other information containers).

186. *See, e.g.*, Martin Lindstrom, *You Love Your iPhone. Literally.*, N.Y. TIMES (Sept. 30, 2011), http://www.nytimes.com/2011/10/01/opinion/you-love-your-iphone-literally.html?mcubz=0.

187. *See, e.g.*, Lawrence Hurley, *U.S. Supreme Court to Settle Major Cellphone Privacy Case*, REUTERS (June 5, 2017), http://www.reuters.com/article/us-usa-court-mobilephone/u-s-supreme-court-to-settle-major-cellphone-privacy-case-idUSKBN18W1RY [https://perma.cc/845E-Z84H?type=image].

188. 425 U.S. 435 (1976).

189. 442 U.S. 735, 743-44 (1979).

190. *Miller*, 425 U.S. at 442-43.

191. *Id.* at 437.

ernment, including deposit slips and personal checks.[192] The Supreme Court determined that no Fourth Amendment interests were implicated because when someone—such as an individual making deposits at a bank—willingly offers up his personal information to a third party, he "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[193] In response, legislation was passed shortly afterwards in the form of the Right to Financial Privacy Act of 1978,[194] which codified a right to protection of one's personal financial records.[195] Outside of such formalized rights, however, offering information to third parties can explicitly surrender an individual's privacy interest in that information. Once that claim of ownership has been apparently relinquished, third parties may legitimately utilize that information or even sell it to others.[196]

Intuitively, people tend to believe that their personal information and intimate facts about them belong to them.[197] However, once shared, third-party nongovernmental entities may also have a right to use, exploit, or sell that information. According to the Supreme Court, "private decisionmaking can avoid governmental partiality and thus insulate privacy measures from First Amendment challenge."[198] In *Sorrell v. IMS Health Inc.*,[199] Vermont's Prescription Confidentiality Law,[200] which put limitations on the sale and use of prescription records, was challenged as unconstitutional under the First Amendment by data miners and pharmaceutical companies.[201] Apparently, it is routine practice for pharmacies and insurers to sell prescriber-identifying information to data miners, including information that pharmacies are required by federal law to record and save when filling prescriptions.[202] The state statute attempted to curb this behavior by making the legality of selling, licensing, or exchanging prescriber-identifying information for marketing purposes con-

192. *Id.* at 438.

193. *Id.* at 443.

194. 12 U.S.C. §§ 3401-3422 (2012).

195. *Id.* § 3402.

196. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 580 (2011).

197. *See generally* MADDEN & RAINIE, *supra* note 10 (discussing how Americans showed overwhelming preferences for controlling who has their information, as well as what happens to it).

198. *Sorrell*, 564 U.S. at 573.

199. *Id.* at 552.

200. VT. STAT. ANN. tit. 18, § 4631 (2010). The law prohibited the sale or use of regulated prescription records kept by doctors, pharmacies, insurers, and employers for marketing purposes without the prescribing doctors' permission. *Id.*

201. *Sorrell*, 564 U.S. at 561.

202. *Id.* at 558.

tingent on first obtaining the prescriber's permission.[203] The Vermont legislature strictly narrowed the scope of the prohibition to the use for marketing purposes, while permitting prescribers to freely disclose information under the statute for research, compliance, or law enforcement purposes—even to pharmaceutical companies and marketers—as long as they did not then use the records for marketing.[204] The Court rejected this approach of relying on private actors—in this case, prescribing doctors—to serve as the gateway for sensitive information disclosure in order to limit a specific use of it, and the state law was found unconstitutional.[205] The Court sustained the lower court's ruling,[206] which held that the Vermont law burdened the commercial speech rights of data miners and marketers under the First Amendment.[207] Data mining and other legitimate exercises of commercial speech rights, like those in *Sorrell*,[208] can significantly complicate and undermine individual privacy rights, especially when personal information is freely given to third parties in exchange for goods or services.[209]

In 2011, in *NASA v. Nelson*, individuals brought suit after being required to submit personal information for a background check, under penalty of termination, to the National Aeronautics and Space Administration (NASA) as part of their contractual employment with the Jet Propulsion Laboratory.[210] While the Court took notice of the potential threat to individual privacy created by the accumulation of personal information, the opinion noted that as explained in previous decisions, a legally imposed duty to keep compiled information secure was generally sufficient to address privacy implications.[211] The Court

---

203. VT. STAT. ANN. tit. 18, § 4631(d) (2010). The state legislature passed the law based on findings that pharmaceutical companies were tailoring their marketing and targeting them at particular doctors largely based on these types of records, and that the pharmaceutical marketing programs have goals directly opposed to the state's interest in effective and affordable prescribing practices. *Sorrell*, 564 U.S. at 560-61.

204. *Sorrell*, 564 U.S. at 580.

205. *Id.* The data miners and pharmaceutical companies argued, and the Court agreed, that their free speech was burdened by the law, based on its content and their identity, which are particularly problematic in the context of burdens on First Amendment rights. *Id.*

206. *Id.*

207. IMS Health Inc. v. Sorrell, 630 F.3d 263, 281-82 (2d Cir. 2010).

208. *Sorrell*, 564 U.S. at 553, 558.

209. Commercial "free speech" and corporate assertions of First Amendment rights have severely curtailed and complicated individuals' rights to privacy, speech, and even health, safety, and welfare, as the government's ability to regulate commerce has been undermined and confined by Supreme Court decisions, such as *Sorrell*, over the last several decades. *See generally* TAMARA R. PIETY, BRANDISHING THE FIRST AMENDMENT: COMMERCIAL EXPRESSION IN AMERICA (2012).

210. NASA v. Nelson, 562 U.S. 134, 138-39 (2011).

211. *Id.* at 155-56.

looked at two decisions from thirty years prior that discussed a privacy right in avoiding the disclosure of personal information.[212] In *Whalen v. Roe*,[213] decided in February of 1977, the State of New York accumulated a record of names and addresses of anyone who had been prescribed certain medications that were known also to be traded in the illegal market.[214] Justice Stevens, writing for the majority, wrote:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy.[215]

This issue again appeared before the Court just four months later in *Nixon v. Administrator of General Services*.[216] Referencing *Whalen*, the Court in *Nixon* again asserted that a constitutional right exists that protects individuals from unwillingly disclosing private, personal information.[217] In 2011, the Supreme Court, after reviewing these two cases, held that the particular background check at issue in *Nelson*[218] did not violate any constitutional privacy right, especially in

---

212. *Id.* at 138.

213. 429 U.S. 589 (1977).

214. *Id.* at 591.

215. *Id.* at 605 (footnote omitted). The Court held that the burden imposed by the potential public disclosure of private health information due to negligence (improper security), need (judicial proceeding), or intention (voluntary disclosure via prescription forms), on "either the reputation or the independence of patients for whom Schedule II drugs are medically indicated is [in]sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment." *Id.* at 603-04.

216. 433 U.S. 425, 425 (1977).

217. *Id.* at 458. The Court, considering the records of the Nixon Administration, found that while the former president had a legitimate expectation of privacy in his personal communications, such as those with his family, doctor, and lawyers, President Nixon's status as a public figure, and the fact that the overwhelming majority of the records were very much of public concern and related to his presidency, negated his privacy claim relating to the process of screening by government archivists of private information from the general disclosure. *Id.* at 461-65.

218. NASA v. Nelson, 562 U.S. 134, 159 (2011).

the face of the government's interests as an employer and the protections provided under the Privacy Act of 1974.[219]

The Supreme Court did at least contemplate a right to informational privacy: "We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*."[220] In the future, constitutional rights concerning personal data will inevitably become more and more important and complex as new and increasingly intrusive forms of information are being analyzed and relied on by both public and private entities and, therefore, in courts of law. For example, the Supreme Court found that swabbing arrestees for DNA samples in order to analyze and compare them against a database of samples, for identification purposes, did not violate the defendant's constitutional rights.[221] As the volume and variety of data being recorded, analyzed, and stored continues to expand, the threat to individual and personal privacy grows concurrently, intensifying the demand for implementation of both traditional protections—such as legislation and regulations—and more modern and novel protections conceivably provided by corporate and private actors.

IV. REGULATING BIG DATA

There are a number of federal laws which apply to personal data, though few, if any, reach the realm of big data and the activities of data brokers. Since the passing of the Privacy Act in 1974, which governs and limits the disclosure of personal information by the government,[222] various legislation has been enacted that regulates the collection and use of personal data both by the public and private sectors. Generally, the security of information collected by the government is assured by federal law through the Federal Information Security Management Act (FISMA), which provides that federal agencies and entities, including government contractors, must implement

219. 5 U.S.C. § 552a (2012); *Nelson*, 562 U.S. at 138. The Privacy Act authorizes the federal government to keep records on individuals only when "relevant and necessary" for a mandated purpose and bars the government from disclosing records on an individual without that individual's written consent. *Id.* at 142; *see also* 5 U.S.C. § 552a(e).

220. *Nelson*, 562 U.S. at 138. Justice Alito, writing for the majority, noted, however, that the Court had not fully considered or affirmed the right to "informational privacy" outside of *Whalen* and *Nixon*, which has been defined as the "individual interest in avoiding disclosure of personal matters." *Id.* at 146 (quoting *Whalen*, 429 U.S. at 599).

221. Maryland v. King, 569 U.S. 435, 465 (2013). As the Court notes in this case, "[a]ll 50 States require the collection of DNA from felony convicts." *Id.* at 445. The Court also held that the government has a legitimate and strong interest in confirming a person's identity, and that persons taken into police custody, despite not yet being convicted or even officially charged, have an obviously diminished expectation of privacy. *Id.* at 462-63.

222. *See* 5 U.S.C. § 552a (2012).

and deploy security provisions.[223] The National Institute of Standards and Technology, through its FISMA Implementation Project, develops the rules and regulations for information security and categorization, and provides guidance on necessary security features and systems required under the statute.[224]

A. Protection for Specific Types of Information

Many federal statutes identify certain kinds of personal information that Congress has classified as necessary to protect, such as data concerning susceptible classes of people (like children) and highly sensitive information (like bank or health records). The Family Educational Rights and Privacy Act (FERPA) protects the privacy rights of students by giving parents certain rights over the education records of their children.[225] As for financial information, the Right to Financial Privacy Act, originally passed as a reaction to the Supreme Court's ruling in *United States v. Miller*,[226] creates protections for bank and financial records.[227] However, the Gramm-Leach-Bliley Act (GLBA), passed in 1999, does permit financial institutions to disclose personal information to affiliated third parties.[228] Where identifiable personal data, like names, telephone numbers, and social security numbers, are associated with health information, the activity falls under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[229] Promulgated under HIPAA, the Privacy Rule and

223. *See* 44 U.S.C. § 3551 (2012).

224. *See* 40 U.S.C. § 11331 (2012); *see also Risk Management—Federal Information Security Management Act (FISMA) Implementation Project*, NAT'L INST. STANDARDS & TECH., http://csrc.nist.gov/groups/SMA/fisma/index.html [https://perma.cc/SV6H-BGPU] (last updated Jan. 8, 2018).

225. *See* 20 U.S.C. § 1232g (2012). Notably, FERPA also covers college campus medical records, and is often less protective than HIPAA. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS. & U.S. DEP'T OF EDUC., JOINT GUIDANCE ON THE APPLICATION OF THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) TO STUDENT HEALTH RECORDS 1-2 (2008).

226. 425 U.S. 435, 1624 (1976) (holding that there was no legitimate expectation of privacy in personal checks and deposit slips because they were voluntarily shared with the bank and its employees and were therefore business, not personal, records). The Court held that the requirement of recordkeeping of checks and deposits by the banks did not negate the voluntary sharing of such information, and therefore, did not create a privacy interest in such records. *Id.*; *see also supra* Section III.B.3.

227. *See* 12 U.S.C. § 3402 (2012).

228. *See* 15 U.S.C. § 6802 (2012). The GLBA requires banks to provide notice and opt-out provisions to consumers, as part of the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012), but exempts certain disclosures, including those related to customer service and marketing by the institution. *See* 15 U.S.C. § 6803(d).

229. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

the Security Rule[230] apply to Protected Health Information, which includes information regarding treatment, status, provider, and payments.[231] The rules outline necessary protections for this sensitive data, whether it is stored physically or electronically.[232]

1. The Collection and Recording of Emails

Formally, the collection and use of email addresses are regulated and limited by applicable federal statutes. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2013 (CAN-SPAM Act)[233] was intended to suppress the inundation of bulk commercial email communications.[234] The FTC notes that beyond spam,[235] the CAN-SPAM Act applies to commercial emails more broadly, including intra-business messages and emailed notices announcing new products.[236] However, the Act has been widely criticized for not only being ineffective but also for preempting more potent state law that could have been enacted absent the federal law.[237] The Electronic Communications Privacy Act (ECPA) also addresses email protection, outlining certain requirements related to search warrants for stored electronic communications;[238] however, the ECPA is seriously outdated[239] and has been further weakened by significant amendments, such as the Patriot Act[240] and its reauthorizations.[241]

---

230. *See* 45 C.F.R. § 164.302 (2016) (Security Rule); 45 C.F.R. § 164.502 (2016) (Privacy Rule) (2017); *see also* OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., HIPAA ADMINISTRATIVE SIMPLIFICATION, REGULATION TEXT, 45 CFR PARTS 160, 162, AND 164 (2013), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf [https://perma.cc/LSD9-C8KD].

231. 45 C.F.R. § 160.103.

232. *See generally* 45 C.F.R. pt. 164.

233. Pub L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713, 18 U.S.C. § 1037 (2012)).

234. *See* Definitions and Implementation Under the CAN-SPAM Act, 73 Fed. Reg. 29,654 (May 21, 2008) (codified at 16 C.F.R. pt. 316) (noting that the Act was intended to create "tools to combat commercial email that is unwanted by the recipient and/or deceptive"); FTC, THE CAN-SPAM ACT: A COMPLIANCE GUIDE FOR BUSINESS 1-2 (2009).

235. Spam is generally defined as unsolicited, commercial emails that are sent to a large number of recipients. *See Spam*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/spam [https://perma.cc/8677-5LS3].

236. *See* THE CAN-SPAM ACT: A COMPLIANCE GUIDE FOR BUSINESS, *supra* note 234.

237. *See, e.g.*, Roger Allan Ford, Comment, *Preemption of State Spam Laws by the Federal CAN-SPAM Act*, 72 U. CHI. L. REV. 355, 357-58 (2005); Jay Reyero, Comment, *The CAN-SPAM Act of 2003: A False Hope*, 11 SMU SCI. & TECH. L. REV. 195, 195 (2007) ("Instead of protecting consumers, it protects commercial marketers; instead of focusing on 'unsolicited' email, it focuses on 'deceptive' email; instead of tackling the problem, it shifts the burden to others; instead of creating a strong legal foundation when preemption occurs, it creates a weak national standard that usurps stronger state initiatives.").

238. 18 U.S.C. §§ 2510-22 (2012).

239. The ECPA was passed in 1986 and has therefore largely weakened privacy protections of emails stored on third-party servers, despite the fact that it is now common prac-

2. Information Relating to Credit Transactions

Where data firms are advising companies on consumer transactions, the Fair Credit Reporting Act (FCRA),[242] as amended by the Fair and Accurate Credit Transactions Act (FACTA),[243] applies. The FCRA governs consumer reporting agencies (CRAs) based on their intricate and inextricable role in commerce.[244] The FACTA requires CRAs to "adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[245] The Fair Information Practice Principles (FIPPs), established by the FTC, reflect the agency's interpretation of what types of activities correspond to reasonable procedures among CRAs.[246] The FIPPs focus are on the principles of notice, choice, access, security, and enforcement for interpreting, regulating, and constraining CRAs behavior.[247] Also, the FACTA features additional safeguards for identity theft, such as requirements to maintain and disclose to the consumer upon request files for fraud-related incidents.[248]

3. Identity Theft

The Identity Theft and Assumption Deterrence Act of 1998 (ITADA)[249] made identity theft[250] a federal offense.[251] The ITADA amended

---

tice to store one's personal emails online, such as on servers owned by companies like Google. *See* Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun By the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html?hp.

240. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

241. *See* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006). *See generally* DEP'T OF JUSTICE, OFFICE OF LEGAL EDUC., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2009).

242. 15 U.S.C. § 1681 (2012).

243. Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified as amended at 15 U.S.C. §§ 1681-1681x (2012)).

244. 15 U.S.C. § 1681(a). CRAs play a significant role in "investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers," and consumer access to the banking system is fundamental to participating in the economy. *See id.*

245. *Id.* § 1681(b).

246. *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (1998); FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000) [hereinafter FTC FAIR INFORMATION PRACTICES].

247. *See* FTC, FAIR INFORMATION PRACTICES, *supra* note 246.

248. 15 U.S.C. § 1681c-1 (2012).

249. 18 U.S.C. § 1028 (2012).

the federal criminal law to make it a crime when someone "knowingly transfers, possesses, or uses . . . a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law or . . . a felony."[252] The Identity Theft Penalty Enhancement Act (ITPEA) offered an aggravated version of the crime, which strengthened the consequences for specific, enumerated felonies, including mail, bank, and wire fraud; obtaining customer information by false pretenses; and making false statements pertaining to social security benefits.[253] Additionally, the ITPEA outlined even stronger sentencing for acts relating to terrorism.[254] According to the FBI, identify theft complaints more than doubled between 2010 and 2015, and the "number of identity theft victims and total losses are likely much higher than publicly-reported statistics."[255]

B. Transparency and Access to Information Held by the Government

To increase government transparency, some federal regulations, however, enable access to information collected and stored by the government. The Freedom of Information Act (FOIA) provides an avenue for individuals to access information held by governmental agencies.[256] With a few exceptions,[257] FOIA requires federal agencies

250. In the context of federal criminal law, the crime of "identity theft" is defined broadly to include possessing, using, or selling false identification, identification of another person, identity authentication features, unauthorized or stolen identification, or equipment for creating false identification, or attempting to do any of the above. *Id.* § 1028(a)(7).

251. *Id.*

252. *Id.*

253. *See* 18 U.S.C. § 1028A(c) (2012). Someone convicted of aggravated identity theft will have a mandatory two-year prison sentence added to whatever other sentencing the court may impose for related crimes. *Id.* § 1028A(a)(1). In addition to those listed above, the aggravated form of identity theft was also tied to crimes related to citizenship, immigration, passports, and firearm acquisition. *Id.* § 1028A(c)(2)-(3), (6)-(7), (9)-(10).

254. *Id.* § 1028A(a)(2). Someone convicted of an act of terrorism who commits identity theft in connection with that act will have a mandatory five-year prison sentence added to whatever other sentencing the court imposes. *Id.*

255. *Identity Theft*, FBI, https://www.fbi.gov/investigate/white-collar-crime/identity-theft [https://perma.cc/P89A-39VV]. The FBI notes that identity thieves use a variety of sensitive information to commit fraud, including: names, Social Security numbers, dates of birth, Medicare numbers, addresses, birth certificates, death certificates, passport numbers, financial account numbers, passwords, telephone numbers, and biometric data such as fingerprints. *Id.*

256. *See* 5 U.S.C. § 552 (2012).

257. *Id.* § 552(e)(1)-(9). The exceptions are for things such as trade secrets, privileged or confidential information, internal memoranda, personnel and medical data, and classified information. *Id.*

to disclose records upon request by the public.[258] Anyone may request records; although, agencies are not required to collect information outside out of their records or reorganize data in response to a request nor are the requests free.[259] Due to the breadth of certain exceptions,[260] the records produced under FOIA may only provide a narrow window of access to the personal information of others; hence, marketers' need for data brokers.[261] Once a private actor has acquired that data, however, it may become available to other sources or compiled with other information, permitting analysis that can expose identifying and sensitive information by combining multiple sources of data.[262]

Recently, this exact issue made headlines when two major events occurred. The first, reported in December 2015, was that a database of seemingly every voter in the United States, including names, birthdates, addresses, phone numbers, party affiliations, and voting history, was discovered to be available on the internet, completely unsecured.[263] The second event occurred following the election of Donald Trump in 2016 when the President established the Presidential Advisory Commission on Election Integrity (Commission) to investigate improper and fraudulent voting.[264] The Commission re-

---

258. *Id.* § 552(a)(3)(A).

259. *Id.* § 552(a)(4)(A)(i); Uniform Freedom of Information Act Fee Schedule and Guidelines, 52 Fed. Reg. 10,012 (Mar. 27, 1987). Under FOIA, its amendments, and related caselaw, there are three classes of requesters (commercial, educational/scientific/media, and everyone else), and three types of fees (search, review, duplication). *Id.* at 10,012-16. However, for noncommercial requesters, agencies are required to provide the first 100 pages of duplication and the first 2 hours of search time free of charge, and there are waivers available for requests that are in the public interest. 5 U.S.C. § 552(a)(4)(A)(iv)(II); *see also* DEPARTMENT OF JUSTICE GUIDE TO THE FREEDOM OF INFORMATION ACT: FEES AND FEE WAIVERS (2014), https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/fees-feewaivers.pdf [https://perma.cc/W67C-XBMG].

260. For example, there are exceptions to FOIA requests for information that is "specifically exempted from disclosure by statute," commonly referred to as Exemption 3 statutes, and exceptions for information that "constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(3), (6); *see also* DEP'T OF JUSTICE, STATUTES FOUND TO QUALIFY UNDER EXEMPTION 3 OF THE FOIA (2016) (listing more than seventy statutes that courts have found qualify under Exemption 3); DEPARTMENT OF JUSTICE GUIDE TO THE FREEDOM OF INFORMATION ACT: EXEMPTION 6, at 417-20, 454-56 (2014) (discussing the balancing test of the privacy interest versus the public interest in determining which information is covered by Exemption 6, by either being an invasion of personal privacy or contained in personnel, medical, or similar types of files).

261. *See* discussion *supra* Section II.A.1.

262. *See* discussion *supra* Section II.B.4.

263. *See* Thomas Fox-Brewster, *191 Million US Voter Registration Records Leaked in Mystery Database*, FORBES (Dec. 28, 2015, 8:50 AM), https://www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/#676a193c5b98.

264. Exec. Order. No. 13,799, 82 Fed. Reg. 22,389 (May 16, 2017) (establishing the Presidential Advisory Commission on Election Integrity); *see also Presidential Advisory Commission*

quested a vast array of voter roll information from all fifty states, including the last four digits of voters' social security numbers, permitting the federal government to create a national database.[265] The aggregation of this sensitive identifying data is concerning to many privacy experts because of the risk of the bulk information being stolen or leaked.[266] Clearly, governmental transparency as afforded by FOIA and similar state and local laws,[267] while certainly positive for democracy, creates a broad source of potentially identifying personal information that can be utilized by individuals and data brokers alike.[268] As far back as 2007, the risk of the combination of voter information with other, more commercial data to create vast databases was well-known and publicly concerning.[269] A decade later, the fact that these databases have only become larger and less secure bolsters the need for explicit solutions to the exponential growth of the aggregation of personal information.

---

on Election Integrity, WHITE HOUSE: BLOG (July 13, 2017), https://www.whitehouse gov/blog/2017/07/13/presidential-advisory-commission-election-integrity [https://perma.cc/R5WR-7ARG].

265. *See, e.g.*, Jessica Huseman, *Presidential Commission Demands Massive Amounts of State Voter Data*, PROPUBLICA (June 29, 2017, 6:00 PM), https://www.propublica.org/article/presidential-commission-demands-massive-amounts-of-state-voter-data [https://perma.cc/VH9N-MSZ7]. The social security numbers, in particular, were seen by states as being nonpublic, and therefore, most states refused the request. *See* Liz Stark & Grace Hauck, *Forty-Four States and DC Have Refused to Give Certain Voter Information to Trump Commission*, CNN (July 5, 2017), http://www.cnn.com/2017/07/03/politics/kris-kobach-letter-voter-fraud-commission-information/index.html [https://perma.cc/VWP5-HC2S].

266. *See* Issie Lapowsky, *Trump Wants All Your Voter Data. What Could Go Wrong?*, WIRED (June 30, 2017, 6:18 PM), https://www.wired.com/story/trump-wants-all-your-voter-data-what-could-go-wrong [https://perma.cc/YE79-SYDZ] ("Aggregating the voter rolls from many states creates a bigger privacy risk than the patchwork of state data we have today . . . ." (quoting Jacob Hoffman-Andrews, Elec. Frontier Found., Senior Staff Technologist)).

267. For example, much of the voter information requested by the Election Commission is publicly available, depending on the state. *See, e.g.*, FLA. STAT. § 97.0525(3)(b) (2017); *Voter Information as a Public Record*, FLA. DEP'T OF STATE, http://dos.myflorida.com/elections/for-voters/voter-registration/voter-information-as-a-public-record [https://perma.cc/7GAY-8CEZ].

268. *See* James Verini, *Big Brother Inc.*, VANITY FAIR (Dec. 2007), https://www.vanityfair.com/news/2007/12/aristotle200712 [https://perma.cc/LLB6-TS53] (discussing the political data broker, Aristotle, who sells huge amounts of voter information, consisting of both public and commercial data, to politicians and others). *See generally* discussion *supra* Part II.

269. Verini, *supra* note 268. The founder of the political data broker, Aristotle, regarding the use of this data to target specific individuals, was quoted as saying:

> I happen to think the rights of the speaker, in the case of political speech, and for the good of society, outweigh the rights of the recipient. . . . The benefits of allowing unfettered debate, even requiring people to hear positions they don't want to hear, outweigh the right of the person to say, "I don't want to hear this."

Id.

V. SOLUTIONS TO THE BIG DATA THREAT

Like the FTC, the White House, scholars, and journalists have noted there are serious potential and realized dangers associated with the ubiquity of the aggregation and use of big data.[270] While it seems that the use of big data in both the private and public sectors will continue, if not expand, in the future,[271] there are numerous potential solutions which can help safeguard personal privacy. Constitutional rights to personal information can be insufficient to protect against these threats,[272] and potential federal legislation, though promising, may be difficult to pass in the current political climate.[273] In addition to legislative efforts, the burden will fall to governmental agencies (through their rulemaking and enforcement activities) and even corporate actors (through their consumer and business practices) to safeguard personal data.[274] In order to address big data concerns, the executive branch should implement more aggressive regulation, which is possible even under existing federal authority,[275] and Congress should pass legislation expanding the scope of federal agencies' power to regulate the movement of information, particularly related to commercial efforts. On the private sector side of the equation, a corporate right to privacy[276] could help ensure the privacy rights of individuals and theoretically protect against governmental intrusion.[277] Similarly, market-based approaches, such as privacy

270. *See* discussion *supra* Section II.B.

271. *See* BIG DATA OPPORTUNITIES, *supra* note 15; Kim Zetter, *Voter Privacy Is Gone—Get Over It*, WIRED (Jan. 31, 2008, 9:18 AM), https://www.wired.com/2008/01/voter-privacy-i [https://perma.cc/C42A-R3P3].

272. *See* discussion *supra* Part III.

273. *See* Andy Greenberg, *Congress Has a Thing or Two to Learn from These State Privacy Laws*, SLATE: FUTURE TENSE (Jan. 26, 2016, 2:49 PM), http://www.slate.com/blogs/future_tense/2016/01/26/electronic_communications_privacy_act_is_due_for_an_upgrade.html [https://perma.cc/AJQ6-D4QF?type=image] (discussing how the eternal gridlock in Congress has caused states to try to respond to the growing privacy concerns with their own legislation); *see also* discussion *infra* Section V.A.2.

274. Companies are known to cultivate their public image and therefore the public's goodwill by protecting their customers' privacy, even in the face of governmental requests for data. *See, e.g.*, Will Oremus, *Apple vs. the FBI*, SLATE: FUTURE TENSE (Feb. 17, 2016, 7:44 PM), http://www.slate.com/articles/technology/future_tense/2016/02/apple_s_stand_against_the_fbi_is_courageous_it_s_also_good_for_apple.html [https://perma.cc/A65R-GX7Z?type=image] (arguing that Apple decided to take a stand against the FBI, even in a case involving terrorism, as an attempt to portray the company as being especially protective of their users' privacy).

275. *See* discussion *infra* Section V.A.1.

276. *See* discussion *infra* Section V.B.1.

277. *See, e.g.*, Kayla Robinson, Note, *Corporate Rights and Individual Interests: The Corporate Right to Privacy as a Bulwark Against Warrantless Government Surveillance*, 36 CARDOZO L. REV. 2283, 2296 (2015) (discussing the positive aspects of a corporate right to privacy, particularly when the right is linked to being good for the public interest). Because so much of our data is held by corporations, and because the Supreme Court has held that

protection services,[278] could assist individuals in ensuring their own personal information is and stays secure.

A. Solutions from the Public Sector

The FTC has the authority to investigate and prosecute companies that participate in unfair or deceptive behavior that has an effect on commerce in the United States.[279] Specifically, under section 5(a) of the FTC Act, the FTC is authorized and directed to prevent corporations "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[280] More aggressive regulation on the part of agencies like the FTC could help deter individual privacy intrusions when constitutional protections fail to do so. Expanding the regulatory impact of such agencies, by growing their regulations to the extent permissible by law, would also allow them to better deal with the ongoing threat of data aggregation and the use of big data.

1. Regulating Within Existing Authority

Some legal experts have suggested that one pathway to addressing the threat of big data to individual privacy is already open to the federal government. In a 2015 law review article, Professors Woodrow Hartzog and Daniel Solove posited that recent cases have exposed the ambiguity of the FTC's authority.[281] Hartzog and Solove argue that the FTC "not only has the authority to regulate data protection to the extent it has been doing, but that it also has the authority to expand its reach much more."[282] The authors contend that the broad domain of authority granted through the FTC Act[283] includes the authority to pursue violations beyond the type of blatant infractions normally investigated and prioritized by the agency.[284]

---

sharing information with third parties "surrenders" one's right to privacy of that information, corporations may be in the best position to protect our information. *Id.*

278. Companies have emerged that scan the internet for a customer's information and attempt to purge information where possible. *See* discussion *infra* Section V.B.2.

279. 15 U.S.C. § 45(a)(1) (2012). The FTC's authority to find practices unfair or deceptive is intentionally broad to permit the FTC's jurisdiction to evolve with time. *See* FTC, FTC Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/V8K2-NM7G].

280. Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2012).

281. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015).

282. *Id.* at 2232.

283. 15 U.S.C. § 45(a)(21).

284. Hartzog & Solove, *supra* note 281, at 2266 (arguing that the FTC's enforcement strategy makes them more "a norm-codifier than a norm-maker").

Further, the authors argue that not only does the FTC have "great potential to regulate data protection with the appropriate nuance and focus,"[285] but that it *should* be exercising its existing authority much more robustly.[286]

There have been several successes in federal regulation which exemplify the possibility of more aggressive regulation not just for the FTC, but for the Federal Communications Commission (FCC) as well. In 2016, for example, the FCC settled with Verizon for $1.35 million over the company's use of tracking cookies without notifying its customers or providing customers with any choices about their data.[287] In 2008, the FTC settled with a credit card company that failed to disclose its use of big data, which reflected a practice of associative discrimination by presuming heightened risk based on similarities between customer spending habits.[288] In 2016, the FTC also settled with the data broker LeapLab in response to allegations that the company (along with others) had sold sensitive information, including banking records and social security numbers, to third parties without customer consent.[289] Both the FCC and the FTC have demonstrated the authority and the ability to go after companies that abuse big data and personal information. However, whether the FCC and FTC are fully able and willing to take similar or more aggressive actions in the future is yet to be seen.

2. Expanding Regulation

In response to wider public knowledge of big data concerns, there are numerous federal and state laws pending across the nation in addition to numerous public- and private-action plans that deal with

---

285. *Id.* at 2299.

286. *Id.* at 2266. Because of rapidly evolving technologies, the clear inability of Congress to pass privacy legislation, and the growing harms caused by big data, the authors argue that the FTC is "one of the best hopes for guiding U.S. privacy law to a more coherent and stable regulatory system." *Id.*

287. Press Release, FCC, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016) [hereinafter FCC Settles Verizon], https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf [https://perma.cc/2NRM-D9F3] (summarizing the FCC's enforcement that included requiring Verizon to inform users of their data tracking practices and to permit users to opt-in and even limit who their data can be shared with).

288. DATA EXCLUSION, *supra* note 34, at 9-10 (citing FTC v. CompuCredit Corp., No. 1:08-cv-1976-BBM-RGV (N.D. Ga. June 10, 2008)).

289. Press Release, FTC, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers (Feb. 18, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive [https://perma.cc/T8KZ-22AM] (summarizing the case, which included findings that LeapLab sold this sensitive information to scammers and telemarketers, who then stole millions from these customers).

big data issues.[290] In 2012, the Obama Administration announced its Big Data Research and Development Initiative,[291] which involved more than $200 million in new commitments to improve big data techniques among federal agencies.[292] Following the 2015 passage of the Cybersecurity Information Sharing Act (CISA)[293] (which received mixed reviews by privacy activists[294]), President Obama announced the Cybersecurity National Action Plan, which is meant to both build a long-term strategy to identify, monitor, and address cybersecurity issues, as well as increase public awareness of cybersecurity issues.[295] Although it is still unclear what position the Trump Administration will pursue, the passage of CISA shows that the government will continue to rely on, and even increase its dependence on, big data analytical tools.[296]

One seemingly simple solution to the threat of big data is to directly address the problem by passing new legislation that more accurately reflects the state of technology in modern America. Unfortunately, this avenue to improve personal data protection can be politically divisive, time intensive, and technically difficult, despite being the traditional method of effecting policy.[297] On March 4, 2015, Senators Ed Markey, Richard Blumenthal, Sheldon Whitehouse, and

---

290. *See, e.g.*, Greenberg, *supra* note 273.

291. Tom Kalil, *Big Data is a Big Deal*, WHITE HOUSE: BLOG (Mar. 29, 2012, 9:23 AM), https://www.whitehouse.gov/blog/2012/03/29/big-data-big-deal [https://perma.cc/3CXZ-MUH5].

292. *Id.* It remains to be seen if the Trump Administration will continue any of these programs, but recent activities have raised doubts. *See, e.g.*, Alina Selyukh, *As Congress Repeals Internet Privacy Rules, Putting Your Options in Perspective*, NPR (Mar. 28, 2017, 6:58 PM), http://www.npr.org/sections/alltechconsidered/2017/03/28/521813464/as-congress-repeals-internet-privacy-rules-putting-your-options-in-perspective (describing a bill passed by Congress and eventually signed into law by the president that repealed a rule passed by the Obama Administration in 2016 that gave consumers more control over how their Internet Service Providers use and share their information).

293. S.754, 114th Cong. (as passed by the Senate, Oct. 27, 2015).

294. *See* Andrea Peterson, *Senate Passes Cybersecurity Information Sharing Bill Despite Privacy Fears*, WASH. POST (Oct. 27, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/10/27/senate-passes-controversial-cybersecurity-information-sharing-legislation [https://perma.cc/ZA4X-GVCB] (noting that privacy activists saw the bill's information-sharing provisions as a "backdoor surveillance bill").

295. Office of the Press Sec'y, The White House, *Fact Sheet: Cybersecurity National Action Plan*, OBAMA WHITE HOUSE ARCHIVES (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [https://perma.cc/JFT4-JP4V] (outlining such initiatives as creating the Commission on Enhancing National Cybersecurity, modernizing government information technology practices, encouraging multi-factor authentication, and investing more federal revenue into cybersecurity).

296. *See* Peterson, *supra* note 294 (noting the law's encouragement of sharing big data to improve security practices and systems).

297. *See* Jonathan Weisman, *In Congress, Gridlock and Harsh Consequences*, N.Y. TIMES (July 7, 2013), http://www.nytimes.com/2013/07/08/us/politics/in-congress-gridlock-and-harsh-consequences.html.

Al Franken introduced a bill called the Data Broker Accountability and Transparency Act.[298] The bill was referred to the Senate Commerce, Science, and Transportation Committee, but had a very low chance of being enacted at the time, and in fact did not pass either house of Congress.[299] The bill would have allowed consumers to access, correct, and block the use of their private information for marketing purposes.[300] It would have also given the FTC explicit authority to create new rules for dealing with data brokers and even create a data hub where individuals could view what personal information was being used by data brokers.[301] While the bill, which focused on accountability and transparency, was supported by privacy groups and nonprofit organizations alike,[302] it failed to gain any real political support or actual traction in Congress.[303]

Similar privacy focused state legislation has been announced throughout the country by private organizations. In January 2016, sixteen states simultaneously announced privacy protection legislation in what the American Civil Liberties Union (ACLU) described as "a nationwide coalition of legislators from both parties and advocacy groups from across the political spectrum."[304] These types of privacy promoting organizations, like the ACLU and the Electronic Privacy Information Center (EPIC),[305] can be influential in Supreme Court

298. S. 668, 114th Cong. (as reported by S. Comm. on Commerce, Sci., and Transp., Mar. 4, 2015).

299. *S. 668: Data Broker Accountability and Transparency Act of 2015*, GOVTRACK, https://web.archive.org/web/20150401234221/https://www.govtrack.us/congress/bills/114/s668 [https://perma.cc/8ACN-4JZR] (according to the archived site, the bill only had a three percent chance of being enacted after it had been introduced during the last session of Congress).

300. *Markey, Blumenthal, Whitehouse and Franken Introduce Legislation to Ensure Transparency and Accountability in Data Broker Industry*, MARKEY.SENTATE.GOV (Mar. 5, 2015), http://www.markey.senate.gov/news/press-releases/markey-blumenthal-whitehouse-and-franken-introduce-legislation-to-ensure-transparency-and-accountability-in-data-broker-industry [https://perma.cc/7FCC-T9RD].

301. *Id.*

302. *Id.*

303. This lack of political will for these types of bills has been shown repeatedly, with previous bills also dying with little to no movement in Congress. *See, e.g.*, Data Broker Accountability and Transparency Act of 2015, S. 2025, 113th Cong. (2014); Data Accountability and Trust Act of 2014, H.R. 4400, 113th Cong. (2014).

304. *Nationwide Effort Aims to Empower Americans to "Take Control" of Their Privacy*, ACLU (Jan. 20, 2016), https://www.aclu.org/news/16-states-dc-introduce-legislation-limit-surveillance-and-protect-student-and-employee-privacy [https://perma.cc/MPM6-GAKM]; *see also #TakeCTRL: Nationwide Privacy Push*, ACLU, https://www.aclu.org/map/takectrl-nationwide-privacy-push [https://perma.cc/NY8P-XALW] (overviewing the range of state legislative efforts to protect personal data, student data, employee data, and location tracking data); Greenberg, *supra* note 273.

305. ELEC. PRIVACY INFO. CTR., https://www.epic.org (last visited July 30, 2017). EPIC states that their mission is to "focus public attention on emerging privacy and civil liberties

cases by submitting amicus briefs outlining often complex and technical issues.[306] These organizations often even have their own initiatives and plans for strengthening personal data rights. EPIC, for instance, launched Data Protection 2016—a campaign dedicated to making data protection policies, such as notice, safeguards, surveillance, and enforcement, a political issue in the 2016 presidential race.[307]

B. Solutions from the Private Sector

The government is not the only entity invested in privacy issues stemming from big data. Corporations rely on big data[308] and, accordingly, have a stake in the comfort of users in disclosing information to them. In February 2016, Apple refused to assist the government in gaining access to a locked iPhone for which the company had designed the operating software and encryption, going so far as to deny a request in the form of a legally issued order.[309] In an open letter to customers, Apple CEO Tim Cook explained why the company was challenging the order.[310] According to Cook, the request to undermine the security of Apple's operating system would set a dangerous precedent and would give the government "power to reach into anyone's device to capture their data."[311]

The letter adopted an overtly patriotic narrative, which served to frame the company's challenge as an action that Apple was forced to take in order to protect the privacy of their customers against an overreaching, uninformed government.[312] On the other hand, the Department of Justice attorneys in the case viewed and insisted that

---

issues and to protect privacy, freedom of expression, and democratic values in the information age." *Id.*

306. *See EPIC Amicus Curiae Briefs*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/amicus [https://perma.cc/QK4Q-5WUD] (listing amicus curiae briefs filed in appellate courts by the EPIC related to issues such as consumer privacy, government surveillance, and the Fourth Amendment).

307. *Data Protection Platform*, ELEC. PRIVACY INFO. CTR., http://dataprotection2016.org [https://perma.cc/EP6J-CZGW] (providing questions to ask candidates to determine their views on data privacy and protections).

308. *See* discussion *supra* Section II.A.

309. Cook, *supra* note 9 (noting that while they complied with the FBI's requests for information, they were refusing to help the government build a backdoor into their iPhone operating system).

310. *Id.* (claiming the FBI had requested that Apple remove certain security features and add new ones to give the government access to essentially all iPhone users' data).

311. *Id.*

312. *Id.* The letter is peppered with allusions to patriotism and constitutional freedoms, using phrases like, "the deepest respect for American democracy" and "love of our country," while describing the government's actions as "an overreach by the U.S. government" that would give the government "the power to reach into anyone's device to capture their data." *Id.*

Apple's refusal was primarily motivated by financial and business concerns with respect to potential harms to its reputation and brand, and they emphasized the national security issues at stake as well.[313] Regardless of the motivation behind Apple's refusal, the company capitalized on the case to not only force a public discussion about the ambiguous legal boundaries surrounding access to corporate data,[314] but also to present itself as a beneficent protector of America's sensitive information.[315] The move gained the support of advocacy groups like the ACLU, who went so far as to file an amicus brief in support of Apple.[316] The organization echoed Apple's concerns that allowing the government to compel Apple in this way would pose a serious threat to personal privacy, making it clear that the ACLU was on Apple's side.[317] In the end, the FBI managed to hack into the iPhone, ending the debate between the principles of privacy versus security without the public or the law actually forming real conclusions.[318] However, when corporations like Apple work in this way to actively guard their customers' privacy, the notion of a corporate right to privacy as an avenue for protection becomes increasingly attractive.

---

313. Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search at 6, *In re* Search of Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

314. Cook, *supra* note 9 (emphasizing that Apple was asking America "to step back and consider the implications").

315. *See, e.g.*, Oremus, *supra* note 274 (referring to Tim Cook's statement as "big, bold, and philosophical, and it sets Apple up to carry what might seem an unlikely banner for a Silicon Valley tech giant: the banner of citizens' right to protect their own data"); Klint Finley, *Apple's Noble Stand Against the FBI is Also Great Business*, WIRED (Feb. 17, 2016, 9:24 PM), http://www.wired.com/2016/02/apples-noble-stand-against-the-fbi-is-also-great-business [https://perma.cc/4Q94-PLK3] ("Apple has been trying to position itself as a protector of privacy, a kind of anti-Google, since long before the FBI's court order.").

316. Brief of Amici Curiae of American Civil Liberties Union, ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties, in Support of Apple, Inc., *In re* Search of Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Mar. 3, 2016).

317. *See* Noa Yachot, *7 Reasons a Government Backdoor to the iPhone Would Be Catastrophic*, ACLU (Feb. 25, 2016, 5:45 PM), https://www.aclu.org/blog/speak-freely/7-reasons-government-backdoor-iphone-would-be-catastrophic [https://perma.cc/5NBU-ZTZX] (arguing that "all those warnings about the end of privacy that may have once sounded hyperbolic will have proved prescient" should the FBI prevail in compelling Apple).

318. *See* Fred Kaplan, *Nobody Won the Apple-FBI Standoff*, SLATE (Mar. 29, 2016, 10:34 AM), http://www.slate.com/articles/news_and_politics/war_stories/2016/03/the_fbi_ended_its_showdown_with_apple_and_neither_won.html [https://perma.cc/2JPP-MN8U?type=image] (arguing that the FBI-Apple showdown ended in bruises for both entities' reputations). The FBI had been seeking a test case for gaining access to Americans' phones, and this one, involving a deceased mass murderer with ties to terrorism, had extremely good optics, so it was a disappointment to drop the case. *Id.* Apple, meanwhile, was on shaky legal grounds and had its reputation bruised when the iPhone software was successfully breached. *Id.*

1. A Corporate Right to Privacy

While the concept of corporate personhood is nothing new in the United States,[319] well-publicized and highly politicized Supreme Court cases in recent years have increased widespread understanding, or at least awareness, of the idea. Corporate personhood is the legal treatment of corporations as people for the purposes of certain constitutional protections.[320] Congress has indicated to the Court that the legal term "person" includes associations, organizations, and corporations.[321] In 2010, the Court heard *Citizens United v. FEC*,[322] a case concerning the permissibility of airing a political advertisement that potentially violated federal campaign law and Supreme Court precedent.[323] Section 203 of the Bipartisan Campaign Reform Act restricted corporate expenditures for political speech that advocates a candidate.[324] The Court, in making its decision, expressly overturned *Austin v. Michigan Chamber of Commerce*,[325] Supreme Court precedent from 1990 that upheld restrictions on corporate campaign advertisements.[326] The Court in *Citizens United* reversed this precedent by a narrow 5-4 margin,[327] holding that the government could not wholly silence political speech, though it could require transparency through disclaimers and spending disclosures.[328] *Citizens United* symbolized a solidification of corporate rights under the First

319. *See* Santa Clara Cty. v. S. Pac. R.R. Co., 118 U.S. 394, 396 (1886). In the headnote to this case, the court reporter proclaimed that the Court was all of the opinion that "[c]orporations are persons within the meaning of the Fourteenth Amendment to the Constitution of the United States." *Id.*

320. *See, e.g.*, Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2766 (2014); Citizens United v. FEC, 558 U.S. 310, 341-43 (2010).

321. 5 U.S.C. § 551(2) (2012) (defining "person" as an "individual, partnership, corporation, association, or public or private organization other than an agency" under federal administrative law).

322. 558 U.S. 310 (2010).

323. *Id.* at 320.

324. 2 U.S.C. § 441b (2012). This effectively banned corporate political speech, and similar laws had been upheld repeatedly in court as permissible campaign regulation to prevent corruption or the appearance of corruption. *Citizens United*, 558 U.S. at 310; *see* Austin v. Mich. Chamber of Comm., 494 U.S. 652, 669 (1990) (upholding a state law banning corporate political expenditures); McConnell v. FEC, 540 U.S. 93 (2003) (largely upholding provisions of the Bipartisan Campaign Reform Act banning certain corporate election expenditures and unlimited donations to political parties).

325. 494 U.S. 652 (1990).

326. *Id.* The Court noted that Michigan's law was aimed at "the corrosive and distorting effects of immense aggregations of wealth that are accumulated with the help of the corporate form and that have little or no correlation to the public's support for the corporation's political ideas." *Id.* at 660.

327. *Citizens United*, 558 U.S. at 393.

328. *Id.* at 371 ("This transparency enables the electorate to make informed decisions and give proper weight to different speakers and messages.").

Amendment,[329] with the Supreme Court clearly and unambiguously stating their position.[330] According to the Court, "[n]o sufficient governmental interest justifies limits on the political speech of nonprofit or for-profit corporations."[331]

Four years later, the Supreme Court again addressed the question of when corporate entities are legally considered persons for the purposes of legal analysis.[332] In *Burwell v. Hobby Lobby Stores, Inc.*,[333] a case concerning legally required insurance coverage for contraception,[334] the Court sparked widespread public controversy and debate about the legitimacy and wisdom of the corporate form being granted rights historically assumed to be restricted to natural persons.[335] The case was another 5-4 split, with the business-friendly majority finding once again that corporations can hold and express rights, including religious expression, even if doing so burdens their employees' rights.[336] The Court found that within the meaning of the Religious Freedom Restoration Act,[337] a corporation could be considered a "person," and its exercise of religion was therefore protected.[338] These cas-

329. U.S. CONST. amend. I.

330. *Citizens United*, 558 U.S. at 372 ("Governments are often hostile to speech, but under our law and our tradition it seems stranger than fiction for our Government to make this political speech a crime.").

331. *Id.* at 364. The Court also noted that corporations "may possess valuable expertise, leaving them the best equipped to point out errors or fallacies in speech of all sorts, including the speech of candidates and elected officials." *Id.*

332. *See* Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2759 (2014).

333. *Id.* at 2751.

334. *See* Patient Protection and Affordable Care Act (ACA), Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of 42 U.S.C. (2012)). Under the ACA, passed in 2010, large employers like Hobby Lobby must provide health insurance coverage that includes free "preventive care" for women, which, through regulations, includes contraception. *Id.*; *see Women's Preventive Services Guidelines*, HEALTH RESOURCES & SERVS. ADMIN., https://www.hrsa.gov/womensguidelines2016/index.html [https://perma.cc/L4BQ-9QBH].

335. *See, e.g.*, Adam Winkler, *Corporations Are People, and They Have More Rights Than You*, HUFFINGTON POST (June 30, 2014, 11:10 AM), http://www.huffingtonpost.com/adam-winkler/corporations-are-people-a_b_5543833.html [https://perma.cc/6WT4-73F9] (arguing that the Court's decision favored a corporation's right to religious liberty over their female employees' right to equal access to legally-mandated health benefits); Binyamin Appelbaum, *What the Hobby Lobby Ruling Means for America*, N.Y. TIMES (July 22, 2014), http://www.nytimes.com/2014/07/27/magazine/what-the-hobby-lobby-ruling-means-for-america.html (arguing that expanding corporate constitutional rights creates a danger that is "not only that corporations can act at the expense of society, but also that the people who control them can act at the expense of their own shareholders, employees and customers").

336. *Hobby Lobby*, 134 S. Ct. at 2785.

337. 42 U.S.C. §§ 2000bb to bb-4 (2012).

338. *Hobby Lobby*, 134 S. Ct. at 2768-69.

es show the proliferating tendency of the current Court to find that corporations are people under the law, with similar rights to individuals.[339]

Some scholars have discussed, in the wake of cases such as *Citizens United* and *Hobby Lobby*, the potential recognition and application of a corporate right to privacy as a limited form of protection against warrantless searches of personal information by governmental actors.[340] In the 2011 case of *FCC v. AT&T Inc.*,[341] however, the Supreme Court found that, for purposes of the Freedom of Information Act (FOIA)[342] at least, corporations could not exercise privacy rights to refuse governmental requests for records.[343] Justice Roberts, who authored the unanimous opinion,[344] wrote:

> We reject the argument that because "person" is defined for purposes of FOIA to include a corporation, the phrase "personal privacy" in Exemption 7(C) reaches corporations as well. The protection in FOIA against disclosure of law enforcement information on the ground that it would constitute an unwarranted invasion of personal privacy does not extend to corporations. We trust that AT&T will not take it personally.[345]

Fueled by the Supreme Court's decisions in *Hobby Lobby* and *Citizens United*, however, some academics have asserted that corporations have a right to privacy, at least when asserting that right would protect records that contain their customers' sensitive personal information.[346] Under this argument, the corporate right to privacy would be a "bulwark" against governmental intrusion.[347] Corporations would, in effect, be expressing the privacy rights of their customers to ensure that governmental searches comply with constitu-

339. *See* Appelbaum, *supra* note 335 (noting that the basic argument is that "corporations, owned by people, should have the same freedoms as people"). The addition in 2017 of Justice Neil Gorsuch will likely exacerbate this trend. *See, e.g.*, Nick Wells & Mark Fahey, *The US Supreme Court is More Friendly to Businesses Than Any Time Since World War II*, CNBC (Mar. 1, 2017), https://www.cnbc.com/2017/03/01/supreme-court-very-business-friendly-data-show.html [https://perma.cc/7WRA-CWD7] (noting that Gorsuch, a very conservative jurist, is likely to make the Court even more receptive to business and corporate interests).

340. *See, e.g.*, Eric W. Orts & Amy Sepinwall, *Privacy and Organizational Persons*, 99 MINN. L. REV. 2275, 2320-21 (2015) (arguing that in addition to or instead of a right to privacy, corporations may have an actual duty to protect the privacy of individuals whose data they collect); Robinson, *supra* note 277.

341. 562 U.S. 397 (2011).

342. 5 U.S.C. § 552 (2012).

343. *AT&T*, 562 U.S. at 409-10.

344. *Id.* at 410 (Justice Kagan took no part in the decision).

345. *Id.* at 409-10.

346. Robinson, *supra* note 277, at 2309.

347. *See generally id.* at 2309.

tional requirements.[348] Other scholars are skeptical that the Court will approve an extension of the constitutional right to privacy to corporations.[349] This skepticism is especially true in light of *FCC v. AT&T, Inc.* and the often-referenced *United States v. Morton Salt Co.*,[350] where the Court held that corporations cannot claim an identical right to privacy as individuals.[351]

Assuming, for argument's sake, that the Supreme Court does recognize a corporate right to privacy, it is not clear how much additional protection, if any, this novel right would provide individuals. Corporations, acting within the legal protections of a right to privacy, could waive their rights, just as individuals may normally waive fundamental constitutional rights.[352] The willful cooperation between corporate actors and governmental agencies in the disclosure of customer information has been well reported.[353] When considering how much faith to place in a corporate right to privacy as a substantial means of protecting privacy, Americans must ask themselves how much they actually trust the corporations with whom they entrust so much data.

---

348. *Id.* at 2319 (noting that a corporate right to privacy could work by "protecting the corporation's stand-alone interests, acting as a check on government surveillance, and protecting the more personal and emotional aspects of the right to privacy of the customers").

349. *See generally* Elizabeth Pollman, *A Corporate Right to Privacy*, 99 MINN. L. REV. 27 (2014) (arguing that while it is an open question whether there is a corporate right to privacy, the Court has been inconsistent in determining when corporate rights normally retained by natural persons are available). Pollman also notes that there is a normative argument against permitting corporations to have unlimited privacy rights, which could create a weapon to "powerfully shield them from investigation or regulation." *Id.* at 31.

350. 338 U.S. 632 (1950).

351. *Id.* at 652 (holding that "corporations can claim no equality with individuals in the enjoyment of a right to privacy").

352. *See* United States v. Olano, 507 U.S. 725, 733 (1993) (discussing how the requirement of an individual holder of a right to personally participate in waiving it, and the procedures necessary for the waiver, are dependent on the right being waived).

353. *See, e.g.*, Spencer Ackermann & Dominic Rushe, *Microsoft, Facebook, Google and Yahoo Release US Surveillance Requests*, GUARDIAN (Feb. 3, 2014, 4:40 PM), http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests [https://perma.cc/TS3R-EFE5]; Michael Riley, *U.S. Agencies Said to Swap Data with Thousands of Firms*, BLOOMBERG (June 15, 2013, 12:01 AM), http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms [https://perma.cc/TNX4-WKK4]. Even in the dispute between Apple and the FBI, Apple willingly turned over other customer data requested by the FBI, as is standard practice among corporations cooperating with law enforcement. *See, e.g.*, Fred Kaplan, *The Battle Between Apple and the FBI Is So Heated Because It's So Unprecedented*, SLATE (Mar. 2, 2016, 11:30 AM), http://www.slate.com/articles/news_and_politics/war_stories/2016/03/the_stakes_in_the_battle_between_apple_and_the_fbi_are_higher_than_you_think.html [https://perma.cc/J38W-7DYV?type=image] (discussing the norm of high levels of corporate cooperation with governmental investigations and law enforcement, including active participation in the NSA's PRISM surveillance program).

Corporate actors do not always appear to be concerned about personal privacy and, to the contrary, they often seem intent on invading it to increase sales.[354] A good example is the 2016 settlement between the FCC and Verizon over the company's use of "supercookies."[355] Verizon, without the knowledge or consent of its customers, inserted supercookies—coded, unique, computer-generated identifiers—into the internet-enabled devices of its users to track their online use, gather information, and deliver targeted ads.[356] Following the FCC's investigation into this behavior, Verizon agreed to conform their practices to a three-year compliance plan, as well as pay a fine of $1.35 million.[357] But despite such outright disrespect for customers, corporations still appear to garner enough trust among customers for them to continue sharing their data.[358]

The 2015 study by the Pew Research Center revealed that, generally, Americans have little confidence in either the government or corporations to keep their data confidential and secure.[359] Numerous news outlet studies and investigations point to similar conclusions, with faint findings that people tend to trust companies more than their own government.[360] It appears that people may trust *some* companies more than the government, [361] or they may *generally* trust companies over agencies,[362] but the general public's confidence in corporations to guard our personal information remains decidedly low.[363] Additionally, internet user polling indicates that while Google ranks

354. This Article is founded on this general assumption, as noted extensively throughout the above text.

355. FCC Settles Verizon, *supra* note 287.

356. *Id.*

357. *Id.*

358. *See generally* MADDEN & RAINIE, *supra* note 10; *see also supra* notes 11-14 and accompanying text.

359. MADDEN & RAINIE, *supra* note 10 at 6-7 (showing between 1% and 9% of the public were "very confident" in either the government or private companies to keep their information secure).

360. *See* Hugh Langley, *When It Comes to Our Data, We Trust Google More Than We Trust the Government*, TECHRADAR (Oct. 7, 2015), http://www.techradar.com/us/news/internet/when-it-comes-to-our-data-we-trust-google-more-than-we-trust-the-government-1305751 [https://perma.cc/F575-NDTG] (noting that in a survey of 3,563 users, 31% of respondents reported that they "trusted the government least with their data"); *It's Your Personal Information. Who Do You Trust with Your Data?*, MYLIFE: BLOG (Aug. 27, 2014), https://www.mylife.com/blog/latest-stories/study-americans-dont-trust-the-people-guarding-their-personal-information (finding that in a survey of 4,000 Americans, Google and LinkedIn were slightly more trusted than the government with customers' personal data).

361. MADDEN & RAINIE, *supra* note 10, at 7.

362. *See* Langley, *supra* note 360.

363. MADDEN & RAINIE, *supra* note 10, at 7 (explaining that 2% of adults surveyed felt "[v]ery confident" in search engine providers to keep data private and secure, and only 1% were "[v]ery confident" in social media websites).

relatively high in data security compared to government and other corporate actors,[364] other companies, such as social media companies like Facebook, are even less trusted than the government.[365] The Pew report indicated that just one percent of adults felt "[v]ery confident" that social media sites would keep records of their online activity secure.[366] TechRadar, an online technology news outlet, and MyLife, a privacy-focused internet company, both conducted studies that found that Facebook was one of the least trusted companies when it came to the handling of personal information and ranked, in both cases, lower than the government.[367] However, this evident lack of trust may not carry much sway with consumers who regularly use and enjoy services like Facebook. As one article reported, the "handling of personal information by private companies is what our readers found most problematic, with nearly every contributor openly distrustful of internet companies, yet with many contributors admitting they use those services regardless of these worries."[368] The seeming discontinuity in people's feelings is understandable. It would be difficult, if not impossible, to participate in modern society without inadvertently and nearly constantly sharing information with corporations and the government.[369]

Edward Snowden, the government contractor who was in many ways responsible for the resurgence in public interest in personal privacy,[370] again joined the privacy discussion in March 2016.[371] Snowden ap-

364. *See* Langley, *supra* note 360 (noting that 10% of respondents trusted Google the least with their data, compared to the 31% that trusted government the least); MYLIFE, *supra* note 360 (noting that 47.2% of respondents in the survey reported that they trusted Google with their information, compared to the 23.2% that trusted the government).

365. MADDEN & RAINIE, *supra* note 10, at 7.

366. *Id.* Only 10% of respondents said that they were even "[s]omewhat confident." *Id.*

367. *See* Langley, *supra* note 360 (noting that 33% of respondents trusted Facebook the least with their data, compared to the 31% that indicated the government; Facebook was found to be the "least trusted" of all the options provided); MYLIFE, *supra* note 360 (noting that 17.1% of those surveyed trusted Facebook with their information, compared to the 23.2% that trusted the government).

368. McMullan, *supra* note 29.

369. *See* Julia N. Mehlman, *If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information*, 81 BROOK. L. REV. 329, 346 (2015) ("Some argue that to participate fully and take advantage of modern, innovative society, one *must* have Internet access.").

370. *See* Lee, *supra* note 78 (discussing, in the days immediately following Snowden's exposure of the program, the revelations about PRISM, the corporate denials of enabling broad surveillance, and the public outcry regarding NSA's seeming invasion of individual privacy).

371. Jon Gold, *Edward Snowden: Privacy Can't Depend on Corporations Standing Up to the Government*, NETWORKWORLD (Mar. 19, 2016, 2:07 PM), http://www.networkworld.com/article/3046135/security/edward-snowden-privacy-cant-depend-on-corporations-standing-up-to-the-government.html [https://perma.cc/QM7Q-8CKR] (noting Snowden argued that not only is unquestioning faith in corporations to protect our privacy ill-advised, but "tech gi-

peared, by video conference, at Free Software Foundation's LibrePlanet 2016 conference, held at the Massachusetts Institute of Technology.[372] At the event, Snowden talked about the willingness with which companies have disclosed information to the government and the dangers of entrusting often-complicit corporations with personal data compared to free software's transparency and openness.[373] In light of the fact that public confidence in companies to act on behalf of their customers is low and the reality that consumers may continue to use the services of companies they do not trust, this warning is certainly reasonable. Certain companies, however, specialize in protecting data for individual users, representing yet another possible solution to threats associated with big data.

2. Market-Based Solutions

> *In a marketplace of ideas where culture is king and data moves faster than people—where scalable opportunities come from turnkey solutions . . . .*
>
> —Actor Max Greenfield as "Schmidt" in FOX's *New Girl*[374]

Another potential piece of the puzzle in the pursuit of protection against the threat of big data is the market's reaction to a perceived need that has yet to be fully served. In response to the monetization of personal data and the emergence of the data broker industry,[375] some companies have emerged that offer services to help customers identify and purge information from accessible online databases. Safe Shepherd, for instance, focuses on types of data that are not as regulated or protected as health or credit information. According to the company:

> Safe Shepherd constantly scans the internet and private databases, looking for your personal information. When we find a company publicizing or selling your personal information, we submit an opt-out request on your behalf, which deletes your record. If a website doesn't allow us to automatically remove your information,

---

ants have already proven more than willing to hand over user data to a government they rely on for licensing and a favorable regulatory climate").

372. *Id.*

373. *Id.* Free software may provide better security because it is more modular and, by being open-source, permits many more users to identify potential weaknesses, as compared to proprietary corporate software. *See, e.g.*, Katherine Noyes, *Why Linux Is More Secure Than Windows*, PCWORLD (Aug. 3, 2010, 11:49 AM), http://www.pcworld.com/article/202452/why_linux_is_more_secure_than_windows.html [https://perma.cc/KM8P-RQLS].

374. *New Girl: All In* (FOX television broadcast Sept. 17, 2013).

375. *See* discussion *supra* Section II.A.2.

> we'll provide straightforward instructions for how to handle the exposure.[376]

The measures taken by Safe Shepherd are intended to guard customer data in the absence of meaningful protection implemented by the government or fostered by public opinion. The company's founder, Robert Leshner, spoke of his company's place in the market during a 2013 interview, saying that, "People think of us as a way of outsourcing their privacy, and so we work on our users' behalf so they don't have to."[377] Leshner went on to remark that his company's approach differed from the techniques used by companies, like Reputation.com,[378] that merely seek to suppress undesirable results.[379] Reputation.com, unlike Safe Shepard, focuses primarily on businesses, not individuals, and operates by soliciting reviews in order to amass positive feedback, leading to improved overall ratings and eventually more business.[380]

Abine is another company that has entered the emerging retail privacy protection market.[381] The company sells smart tools for consumers to actively protect their own personal data.[382] Abine's primary products are Blur, which protects information at its originating point (the user's input device), and DeleteMe, which removes information at its assorted termini.[383] Blur generates, secures, and synchronizes passwords across devices;[384] provides masked emails, an option where customers may submit an alias email address (generated and secured by Abine), to help avoid the unwanted dissemination of their account information;[385] creates masked cards, which similarly hide real credit card information from online transactions by automatically generating a temporary credit card number;[386] and overall works to diminish

376. SAFE SHEPHERD, https://www.safeshepherd.com/how (last visited July 30, 2017).

377. Erin Barry & Joanna Weinstein, *Tackling Internet Privacy: Safe Shepherd Joins the Fray*, CNBC (Apr. 16, 2013, 12:11 PM) (quoting Robert Leshner), http://www.cnbc.com/id/100645791 [https://perma.cc/C5QM-Y9ZJ].

378. REPUTATION.COM, https://www.reputation.com (last visited July 30, 2017).

379. Barry & Weinstein, *supra* note 377.

380. REPUTATION.COM, *supra* note 378.

381. ABINE, https://www.abine.com (last visited July 30, 2017).

382. *Id.*

383. *Id.*

384. *Let's Talk About Passwords*, ABINE, https://dnt.abine.com/#feature/passwords [https://perma.cc/MS84-64ER?type=image].

385. *Masked Information*, ABINE, https://dnt.abine.com/#feature/masking [https://perma.cc/P2VC-ASGJ?type=image].

386. *Blur—Masked Cards—4 Simple Steps*, ABINE, https://dnt.abine.com/#feature/payments [https://perma.cc/2L4N-7ZTS?type=image].

methods of tracking online activity.[387] Blur focuses on protecting private data at its source, where it is being created, by masking information submitted to third parties and by securing user data through advanced encryption techniques.[388] Abine's other major product, DeleteMe, on the other hand, focuses on information that is already published online.[389] The service removes publicly available information—including contact information, social media use, and personal photos—from people search sites, like the ones suggested in the introduction, and other data-collecting sites[390] by sending opt-out requests on behalf of its users.[391] Unfortunately, this removal is limited. According to Abine, DeleteMe cannot remove information from websites that do not provide an opt-out capability (many of which are outside of the United States), and the service cannot affect Google search results.[392]

Privacy protection companies operate in the context of particularly troublesome issues, such as the relative ease with which data can be duplicated and the increasingly permanent nature of digital data itself.[393] In fact, this difficulty is progressively becoming an issue in law enforcement, where the digital duplication of suspects' personal computer devices raises similar privacy concerns.[394] Even if privacy protection companies were successful in eliminating all of the available online data published on an individual, which by their own admission is not possible,[395] this would not affect unpublished information held by data brokers, nor would it alter accessible website backups, such as those available online through archival efforts, like the nonprofit, Internet Archive.[396]

The services that companies like Safe Shepherd and Abine provide present unique market-based approaches to supplementing personal data protection. Somewhat ironically, these solutions involve a user

---

387. *So Who Are These Tracking Companies?*, ABINE, https://dnt.abine.com/#feature/tracking [https://perma.cc/XN36-CY2S?type=image].

388. ABINE, *supra* note 381.

389. *DeleteMe*, ABINE, https://www.abine.com/deleteme [https://perma.cc/PSD4-LVCX?type=image].

390. *See supra* notes 63-71 and accompanying text.

391. *DeleteMe Frequently Asked Questions*, ABINE, http://www.abine.com/deleteme/faq [https://perma.cc/24FZ-T782].

392. *Id.*

393. BIG DATA OPPORTUNITIES, *supra* note 15, at 9 (noting that big data has proliferated as data storage has become so ubiquitous and inexpensive).

394. *See* Note, *Digital Duplications and the Fourth Amendment*, 129 HARV. L. REV. 1046, 1047 (2016) (noting, perhaps alarmingly, that "it is not entirely settled that the government conducts either a search or a seizure when it makes a copy of locally stored data").

395. *See DeleteMe Frequently Asked Questions*, *supra* note 391.

396. INTERNET ARCHIVE, http://archive.org/web (last visited July 30, 2017).

paying one company (a privacy protection company) to remove data from a second company (a data broker or people search website) that is already profiting from collecting, selling, or publishing the user's data, and who may have acquired the data from a third company (an online retailer or other corporation), who also profited from the user at the point of the data origination. All three companies in this scenario profit from the receipt or sale of the user's data, while the user is left paying more than assumed or often disclosed, in the form of personal information, for the privilege of shopping online. Additionally, pay-for-privacy solutions inevitably favor those who can afford the services, fostering economic inequality in the protection of individual privacy and from various types of fraud.[397] The problem may simply be too large and pervasive for both individuals and smaller private businesses to tackle alone.

VI. CONCLUSION

There are many possible avenues available for addressing the threat to Americans' privacy represented by the massive accumulation and aggregation of personal data. Data brokers, as the poster children for big data, challenge the boundaries of what constitutes an invasion of privacy in the eyes of the Supreme Court, and their enduring lack of regulation suggests that solutions must also be found elsewhere. However, it is still imperative that governmental agencies, such as the FTC, pursue more robust and aggressive regulation within their existing authority, and that Congress enact broader grants of executive authority and legal protections through new legislation to help disincentive and discourage improper use, or misuse, of personal data. An established corporate right to privacy has potential also to offer some protection for individual consumers from governmental intrusion, although the possibility that such protection could be waived and the risks inherent in expanding corporate constitutional rights are serious and should not be ignored. As corporations increasingly present themselves as self-appointed guardians of personal data, a corporate right to privacy could form another barrier to intrusion on the privacy of consumers, but this would still depend on consumer trust in these companies. In the meantime, companies like Safe Shepherd and Abine offer alternative solutions to impede or at least curtail the onslaught of personal information collection and aggregation.

397. Notwithstanding that many of these companies do offer some services for free through limited-time trials. *See, e.g.*, *Try Safe Shepard Completely Free for 10 Days*, SAFE SHEPHERD, https://www.safeshepherd.com/signup [https://perma.cc/ACL6-SUHT] (offering a free 10-day trial); ABINE, *supra* note 381 (offering a free account with limited features).

The trend of big data usage will likely continue to proliferate, with both governmental and corporate actors relying more heavily on the analytics and insights it provides in their decisionmaking, policymaking, and marketing strategies. Unregulated data brokers will also almost definitely continue to build and sell vast, complex, and increasingly comprehensive datasets on individuals. Additionally, more and more companies are likely to collect information from their customers with the intention of later profiting from the sale of that data. As long as consumers continue to share information in exchange for services, and every indicator suggests they will, the threat posed by the galaxy of personal information will escalate. This is a policy area where there is a clear and identifiable threat to the American people, an issue the people themselves are legitimately and transparently incapable of solving on their own. Given the general public's low confidence in both public and private actors responsible for and active in data collection and use, this is an apparent opportunity for both public and private actors to act decisively and aggressively to regain the trust and goodwill of the people. Through a multipronged approach, via stronger regulation, new legislation, assertion of corporate rights, *and* market-based solutions, the government and corporations alike have the ability and obligation to safeguard the people by becoming true guardians of the galaxy of personal data.