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

Timothy A. Asta[*]

Florida State University College of Law
Spring 2016 – Professor Garrick Pursley
Corporations and the Constitution

[*] Juris Doctorate Candidate, Florida State University College of Law.

TABLE OF CONTENTS

> 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*

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 own name and look at the results. What you will find is not just the result of the website query, but in fact the result of modern big data collection and analytics. The aggregation of personal information presents unique and often vague threats to personal privacy,[7] potential harms that the protections guaranteed by the Constitution, as interpreted by the Supreme Court, seem insufficient to guard against.[8] Perhaps corporations, not the government, would be more effective at ensuring the fidelity and the security of consumer information. Recent corporate actions and announcements would suggest that corporations are eager to take on the impetus of data protection and crown themselves guardians of our personal data. For example, Apple recently refused to comply with an official legal order to unlock an iPhone, an action which, in their view, risked the privacy and security of their customers.[9] This refusal could signify a change in the environment of personal privacy. As companies, like Apple, present themselves as the proper entities to watch over our

[1] John Perry Barlow, *Decrypting the Puzzle Palace*, 35 COMMUNICATIONS OF THE ACM 25, 25 (1992).
[2] President Barack Obama, An Honest Government, a Hopeful Future, Address to the University of Nairobi (Aug. 28, 2006), https://www.whitehouse.gov/the-press-office/2015/07/26/remarks-president-obama-kenyan-people.
[3] SPOKEO, http://www.spokeo.com (last visited May 8, 2016).
[4] PEOPLE LOOKUP, http://www.peoplelookup.com (last visited May 8, 2016).
[5] PRIVATE EYE, http://www.privateeye.com (last visited May 8, 2016).
[6] PUBLIC RECORDS NOW, http://www.publicrecordsnow.com (last visited May 8, 2016).
[7] *See* discussion *infra* Part I.
[8] *See* discussion *infra* Part II.
[9] Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter.

data, 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, and even less confidence was reported when dealing with cellphone companies, email providers, and online websites.[14]

If the American people have almost equally-low confidence in corporations and governmental agencies, then perhaps both entities would benefit from taking action which would garner confidence among the public. This paper examines the relevant threat that big data, and data brokers in particular, poses to the privacy of individuals and what, if any, constitutional rights protect the privacy of personal information. Four possible solutions are considered as potential avenues to challenge the threat. These solutions, offered by the public and private sectors, are: more aggressive regulation under existing statutory authority, expanding the authority of agencies to regulate through new legislation, the possibility of a corporate right to privacy as a barrier to governmental intrusion, and market-based solutions as small-scale techniques 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, though none by itself is sufficient. However, through a holistic approach utilizing all of these solutions, personal information can become less accessible to

[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.

undesired recipients, more secure and accurate for desired applications, and more transparent to the individual whose data it was in the first place.

Part I examines the threat that the accumulation of information presents and the effect on personal privacy by the industry of data brokers which has grown 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 largely unregulated, industry that indiscriminately sells information about private citizens.

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

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

Part IV identifies and analyzes potential solutions, from both governmental and corporate entities, to the 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 section 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.

Part V briefly summarizes and concludes the article, while suggesting that a holistic 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 following the revelation that agencies were conducting 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 engender confidence among consumers. This approach ensures that, regardless of who our guardians are, our personal information remains well-protected.

I. THE BIG DATA THREAT TO PERSONAL PRIVACY

The accumulation of personal information, and in particular the abuse of big data, poses a significant threat to the privacy of individual consumers. Due to technological advances in collection, storage, and utilization of data, the sheer volume of information being aggregated today is unprecedented.[15] Particularly sensitive data, such as federal tax information, social security numbers, and credit reporting, is strictly monitored and regulated. The Fair Credit Reporting Act (FCRA),[16] for example, governs the use of consumer information by credit reporting agencies.[17] Most activities performed by data brokers and other companies that utilize big data, however, fall outside of scope of the FCRA.[18] Outside of this act, there is no federal regulation governing the collection of personal data that directly applies to the largest of all information aggregators, data brokers.[19] The threat to consumers, unfortunately, is not so easily severed once credit sensitive information is eliminated from the analysis. The aggregation of less-sensitive information still poses a distinct and potent threat to individual privacy, one exasperated by the data broker industry and only minimally addressed by the government.

A. The Aggregation of Personal Information

The corporate desire for aggregated information is palpable, with an expanding online market place demanding increasingly accurate consumer information to target a diverse and unsorted mass of users.[20] America's ever-increasing dependence on the digital, rather than the physical, storage of information has resulted in an unprecedented accumulation of personal information.[21] According to the Supreme Court, the "capacity of technology to find and publish

---

[15] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 4 (2014) [hereinafter BIG DATA OPPORTUNITIES].
[16] 15 U.S.C. § 1681 (2014).
[17] *Id.*
[18] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at i (2014) [hereinafter DATA BROKERS].
[19] *See* discussion *infra* Part III.
[20] *See generally* BIG DATA OPPORTUNITIES, *supra* note 15.
[21] *See, e.g.*, *Big Data and the Future of Privacy*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/big-data (last visited May 8, 2016) (Google processes thousands of times more data in a day than exists in the entire printed material of the U.S. Library of Congress); *What is Big Data?*, IBM, http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (last visited May 8, 2016) ("90% of the data in the world today has been created in the last two years alone").

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."[22]

Social interactions are increasingly reliant on third parties to foster both personal and business relationships. Companies search for employees online, while employees look for jobs there too. Sites like LinkedIn provide networking opportunities, and having a business profile or resume online is becoming commonplace.[23] Facebook keeps individuals from being uniformed of, or inadvertently excluded by, their social group,[24] and Twitter[25] breaks news faster than any other news source.[26] All of these services come with a price, but that price is not paid upfront. Instead, payment is generally made in two ways: advertising and information. Advertising is by far the more apparent of the two, making itself immediately clear to users via onscreen commercials and online ads. The part that most people are unaware of is the gathering of information, the use, and the sale of their information for purposes like marketing and publishing.[27] And even when they are aware of this price, many continue to use the services regardless.[28]

1. "Big Data"

The Federal Trade Commission (FTC) notes that in "today's economy, Big Data is big business."[29] But what is "big data" and why is it important? The term, big data, is largely undefined and varies depending on industry, but generally the definition involves the collection of large volumes of complex, structured datasets that are sifted via some form of technology.[30] 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."[31] Big data

---

[22] Sorrell v. IMS Health Inc., 564 U.S. 552, 579 (2011).
[23] LINKEDIN, https://www.linkedin.com (last visited May 8, 2016).
[24] FACEBOOK, https://www.facebook.com (last visited May 8, 2016).
[25] TWITTER, https://twitter.com (last visited May 8, 2016).
[26] *See* Barry Ritholtz, *How Twitter Is Becoming the First and Quickest Source of Investment News*, WASH. POST (April 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.
[27] DATA BROKERS, *supra* note 18.
[28] *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.
[29] DATA BROKERS, *supra* note 18.
[30] [illegible]ard & Adam Barker, *Undefined By Data: A Survey of Big Data Definitions*, ARXIV [illegible] 821 (2013), http://arxiv.org/abs/1309.5821.
[31] BI[illegible]A OP[illegible]ITIES, *supra* note 15, at 2.