12-2016

Protecting One's Own Privacy in a Big Data Economy

Anita L. Allen
University of Pennsylvania Carey Law School

LAW, PRIVACY & TECHNOLOGY COMMENTARY SERIES

PROTECTING ONE'S OWN PRIVACY IN A BIG DATA ECONOMY

Anita L. Allen[*]

I. INTRODUCTION: BIG DATA AS A PRIVACY PROBLEM

"Big Data" are two small words with enormous societal meaning.[1] The words signify a complex phenomenon that has come to define the second decade of the twenty-first century. Big Data is the vast quantities of information amenable to large-scale collection, storage, and analysis. Using such data, companies and researchers can deploy complex algorithms and artificial intelligence technologies to reveal otherwise unascertained patterns, links, behaviors, trends, identities, and practical knowledge. The information that comprises Big Data arises from government and business practices, consumer transactions, and the digital applications sometimes referred to as the "Internet of Things."[2] Individuals invisibly contribute to Big Data whenever they live digital lifestyles or otherwise participate in the digital economy, such as when they shop with a credit card, get treated at a hospital, apply for a job online, research a topic on Google, or post on Facebook.

Representing the push to collect massive amounts of analyzable data for the purpose of discerning valuable information, Big Data presents major challenges to the ideal of personal privacy, which includes rights of limited access to personal information and control over personal information.[3] Privacy advocates and civil libertarians say Big Data amounts to digital surveillance that potentially results in unwanted personal disclosures, identity theft, and discrimination in con-

---

[*] Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania Law School.

[1] *See* DAVID BOLLIER, THE PROMISE AND PERIL OF BIG DATA (2010), https://www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf [https://perma.cc/CD6F-ACYZ].

[2] The popular term "Internet of Things" designates the result of connecting everyday tools and appliances — like heating systems, refrigerators, and FitBits — to the internet to improve their accessibility and function. *See* Jacob Morgan, *A Simple Explanation of "The Internet of Things,"* FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#4a6ee29b6828.

[3] *See generally* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/JE9Y-BJ3B] (discussing privacy concerns stemming from the rise of Big Data and issuing policy recommendations).

texts such as employment, housing, and financial services.[4] These advocates and activists say typical consumers and internet users do not understand the extent to which their activities generate data that is being collected, analyzed, and put to use for varied governmental and business purposes.

I have argued elsewhere that individuals have a moral obligation to respect not only other people's privacy but also their own.[5] If the experience of privacy is important to human dignity and wellbeing, it is something individuals with a choice should not choose to carelessly discard or give away. We must protect our own data to the best of our abilities. Our often-overlooked ethical responsibility to do so could entail circumspect use of social media and credit cards, along with diligent use of passwords, encryption, and security software to limit access to devices. Here, I wish to comment first on whether there is an ethical obligation to protect one's own privacy; second, on whether the notion that individuals have a moral obligation to protect their own information privacy is rendered utterly implausible by current and likely future Big Data practices; and finally, on whether a conception of an ethical duty to self-help in the Big Data context may be more pragmatically framed as a duty to be part of collective actions encouraging business and government to adopt more robust privacy protections and data security measures.

II. AN ETHICAL OBLIGATION TO PROTECT ONE'S OWN PRIVACY

Philosophically speaking, protecting data privacy should be understood as an ethical responsibility of good governments, businesses, and individuals. Ideals of rights, justice, and moral respect pervasively call upon us to regulate access to personal information. Federal and state privacy laws appropriately aim at such ends. Indeed, privacy is so important that good government is warranted in protecting forms of privacy that some individuals do not themselves value.[6] While much of moral life relates to how we treat other people, it also relates to how we treat ourselves. The Kantian deontic moral tradition, for example, asks us to respect our own humanity, for we are owed respect as rational beings with moral autonomy. My views about moral duty are

---

[4] *See, e.g.*, MARC ROTENBERG ET AL., ELEC. PRIVACY INFO. CTR., COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER TO THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY: REQUEST FOR INFORMATION: BIG DATA AND THE FUTURE OF PRIVACY 2–6 (2014), https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf [https://perma.cc/ZQJ9-L8EW].

[5] *See* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845 (2013).

[6] *See generally* ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (exploring the plausibility of paternalistic privacy policies within liberalism).

influenced by this tradition. The German philosopher Immanuel Kant derived duties to others and to oneself from a general moral law — a categorical imperative — to "act that you use humanity, whether in your own person or in the person of any other, always at the same time as an end, never merely as a means."[7] Extrapolating from Kant's categorical imperative, I have elsewhere argued that "[d]uties to oneself are duties of self-care and self-respect" to act "with self-regard, dignity, and integrity," and "to promote one's rational interests in security, freedom, and opportunity."[8] I believe duties to the self of self-care and self-respect entail reservation and circumspection when it comes to sharing potentially sensitive information and the intimacies of identity and personality.[9] And while the case for protecting one's own privacy can be made in Kantian terms, one could also build a case for limiting disclosures of information about oneself on moral utility grounds, stressing moral interests in protecting reputation and future opportunity, and on moral virtue grounds, pertaining to modesty, reserve, and temperance as important character traits. Thus, while business and government owe us privacy, we also owe ourselves privacy.

There are serious practical limits to protecting our own privacy. The methods of data collection and analysis associated with Big Data represent challenges to individuals' capacity to make meaningful privacy-protective interventions. Typical individuals among us, even the well-educated, are technologically unsophisticated, and the cultural and economic pressures to engage in transactions that call for information disclosures are great. Moreover, individuals do not and cannot effectively negotiate over privacy-related "terms and conditions" to ensure privacy advantages. What then, in the Big Data era, might be the content of any moral responsibility to protect one's own privacy? It looks empty. Protecting our own information privacy seems like a manageable task when we focus on such commonplace activities as being more reserved in conversation, using passwords on electronic devices, installing security software, encrypting, and moderating use of social media. Easy self-protection also includes not opting out of our employers' institutional firewalls that monitor internet traffic to repel known threats. Those kinds of activities have a role but are not capa-

---

[7] IMMANUEL KANT, GROUNDWORK OF THE METAPHYSICS OF MORALS 4:429 (1785), *reprinted in* PRACTICAL PHILOSOPHY 37, 80 (Mary J. Gregor ed. & trans., 1996). In an alternative formulation, Kant advanced that a person should "act only in accordance with that maxim through which [the person] can at the same time will that it become a universal law." *Id.* 4:421, at 73 (emphasis omitted).

[8] Allen, *supra* note 5, at 854.

[9] *See id.* at 863–65 (arguing that the concept of duties to the self are plausible and conceivably include duties to protect one's own privacy).

ble of delivering robust information privacy. Big Data is an ethical game changer since there can be no ethical duty to do the impossible.

III. TAKING RESPONSIBILITY: TO EMBRACE OR TO FIGHT BIG DATA?

At present, Big Data can feel like Big Brother, a natural enemy of personal privacy and free choice. Ascribing an obligation of protecting our privacy seems to require something exceedingly difficult or impossible: the eschewal of activities that contribute to the production of massive data sets and analysis. Individuals are generously feeding Big Data. Currently, Big Data analytics involve unknown and nonconsensual uses of data generated by individual conduct that may reveal behaviors and identities to individuals' detriment. Two possibilities merit exploration: that Big Data ought not to be constrained by individuals and that Big Data cannot be constrained by individuals.

One possibility is that any moral responsibility to protect one's own privacy does not include an obligation to constrain Big Data because Big Data's beneficial uses for commerce, security, and public health and safety override privacy concerns. The claim that technology is a net privacy boon is a familiar one. In the early days of the internet it was common to point out that technology could increase privacy. For example, it was argued that with the internet, one would be able to shop without going out into town, read a new book without visiting a brick and mortar library or retailer, and communicate with friends and strangers anonymously. Today we know that we are not invisible as we shop, read, and converse online and that we can be held accountable.[10] The internet of the 1990s was not quite the privacy boon it first appeared to be. Yet maybe Big Data is different. Perhaps Big Data, the "greatest tsunami of information that humans have ever seen,"[11] will net major privacy-related benefits.

While collecting detailed information about us, Big Data might lead to the discovery of new ways to limit access to persons and personal information and create opportunities for an enhanced and less accountable personal life. Focusing on medicine and health as an example, self-tracking made possible by Big Data could improve preventive medicine, increase autonomy, and keep us away from hospitals, therapists, and the like.[12] For instance, if Big Data analytical results show that less expensive home care is superior to expensive hospital

---

[10] *See, e.g.*, Doe I v. Individuals, 561 F. Supp. 2d 249, 257 (D. Conn. 2008) (ordering the unmasking of an anonymous AutoAdmit.com discussion board poster who defamed and invaded the privacy of female Yale Law School students).

[11] Juan Enriquez, *Reflections in a Digital Mirror*, *in* THE HUMAN FACE OF BIG DATA 18, 21 (Rick Smolan & Jennifer Erwitt eds., 2012).

[12] *Id.* at 34.

stays for certain classes of patients, that could be a boon to privacy and could lead to cost savings. Similarly, Big Data results could uncover ways to give people with disabilities more personal independence. In a different context, it potentially would allow police departments to identify police officers at risk of serious misconduct and impose interventions. Furthermore, some of the things we do in our private lives may be better done someday because of Big Data: choosing a partner, buying a new home, planning a long vacation, and passing our native languages along to our children, to name a few. In being constructively critical of Big Data's threats to our privacy, we should also be aware of these potential advantages and encourage government and business to foster uses of Big Data that may support important privacy interests. Big Data feels like a threat to privacies we should care about, such as medical and financial privacies, but perhaps Big Data could — or even already does — have a net positive effect on privacy. Technological developments may compromise privacy and security, but technological innovation might also contribute to a greater degree of privacy in the long run.

From this point of view, individuals would actually harm themselves and others if they succeeded at putting Big Data on a serious diet by generating less data to sustain it. In this vein, one commentator argues that "[t]here's an 'obsession around the issue of privacy' that has sometimes 'derailed' efforts to use data to address critical issues such as combating child abuse, improving education and life-saving medical research."[13] Are there "communities where not enough data — or not enough good quality data — is being collected"?[14]

Yet absolute deference to the common good is inconsistent with the Western morality of individual rights and responsibilities. Being a moral person with rights stems from a conception of human dignity whereby we are not utterly at the disposal of others, existing for their use and to serve their ends. We are subjects, not mere objects; we are entitled to have our own ends take priority over others' in a robust range of circumstances needed to respect our autonomy and welfare. The goal should thus not be to deny privacy but rather to find the sweet spot between public and private good and to understand the extent to which privacy is itself also a public, communal good.

---

[13] Dibya Sarkar, *"Obsession" Around Privacy Said to Affect Big Data Collection but Some Say It's Warranted*, COMM. DAILY (June 23, 2016), http://www.communicationsdaily.com/article/view?s=117058&p=1&id=497461 (quoting Daniel Castro, Vice President of the Information Technology and Innovation Foundation).

[14] *Id.* (discussing Castro's demographic concerns regarding the impact of Big Data on Hispanic Americans and the LGBT community, whose data are not collected as well or often as that of other groups).

A second possibility is that our privacy claims are not all overridden by the promise of Big Data to make the world better and that we have a moral obligation to try our best to constrain Big Data for the sake of our privacy. Our moral efforts might begin with more careful reflection on our habitual daily practices at home or at work and their deep ethical significance, both personal and communal.[15] Yet third-party collection and use of data is mostly invisible to ordinary people. Moreover, it is one thing to put up a curtain in one's bedroom and limit use of social media, but it is something else to be savvy about the ways in which contemporary lifestyles and business practices generate tiny bits of data, some seemingly insignificant, that can be collected, aggregated, and analyzed to reveal patterns, preferences, and identity. The capacity of individuals qua individuals to take steps in daily life to limit Big Data's ability to capture data is limited by deficits of knowledge and practical alternatives. Holding individuals responsible for something they can do nothing about makes little sense, raising the specter that Big Data leaves us helpless to meaningfully protect our own privacy and secure our own information.

IV. ACTING INDIVIDUALLY, ACTING COLLECTIVELY

Individuals can act collectively to constrain and improve Big Data practices. The moral obligation to protect one's own privacy remains a meaningful concept so long as one recognizes that the obligation requires participating in the political process and supporting consumer activism and advocacy, as well as making adjustments in one's own individual behavior and family education. Collectively, individuals can push for reforms and be critical of government.

There is much of which to be constructively critical. In response to a legislative draft of a Privacy Bill of Rights promulgated by the White House, Jeff Chester of the Center for Digital Democracy opined that in a world in which "[t]here's no meaningful consumer control

---

[15] *See, e.g.*, GIORGIA LUPI & STEFANIE POSAVEC, DEAR DATA (2016) (recounting authors' yearlong exchange of postcards detailing minute aspects of daily life such as purchases and emotions that in aggregate reveal important aspects of personality and identity); *see also* David Silverberg, *The Minute Data of Everyday Life on 52 Postcards over 52 Weeks*, WASH. POST (Aug. 27, 2016), https://www.washingtonpost.com/entertainment/books/the-minute-data-of-everyday-life-on-52-postcards-over-52-weeks/2016/08/24/39e2b4d6-689e-11e6-ba32-5a4bf5aad4fa_story.html [https://perma.cc/23FT-ML6F] ("We live in a world obsessed with big data. Algorithms and apps detect and aggregate every bit and byte of information passing through our online and offline interactions. Analytics increasingly inform us about user behavior in real time. But 'Dear Data' harks back to a more nostalgic era when we deliberated over the information we took in and offered to others. Let's call it Slow Data. 'To draw is to remember,' the authors write, and their book reminds us that physical documents can be a time capsule we continually pore through long after Facebook and Instagram have made way for the next Internet flavor of the month." (quoting LUPI & POSAVEC, *supra*)).

of . . . data" nor of "intimate details about people's lives," the White House draft just "makes big data even bigger as it allows the current collection of data to continue."[16] The recommendations in a recent White House report on addressing Big Data challenges do not call for major new legislative agendas.[17] There is the mere hint that government and private sector rules are called for, along with other solutions.[18] Some of the most vocal critics of Big Data call for much more, from an entire EU-style overhaul of current national privacy law,[19] to changes in existing sectorial statutory frameworks like the Health Insurance Portability and Accountability Act[20] (HIPAA) or structures of regulatory agency responsibility for consumer protection,[21] such as protection by the FTC or the FCC.[22] Meriting praise is a recommendation of the federal Big Data Research and Development Strategic Plan for more "Big Data ethics research" comparable to the ethical, social, and legal implications research that has been a part of the government's genomics and nanotechnology initiatives.[23]

There are many other voices and initiatives that are worth supporting in the collective effort to protect individual control over privacy. An emerging perspective that seeks to reconcile privacy and Big Data argues that Big Data will not achieve its aims unless something can be

---

[16] Katie Rucke, *House Privacy Caucus Panel Debates White House Consumer Privacy Bill of Rights Legislative Draft*, COMM. DAILY (Mar. 18, 2015), http://www.communicationsdaily.com/article/view?s=117061&p=1&id=462588 (discussing Chester's concerns regarding the bill).

[17] *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS (2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf [https://perma.cc/H7JQ-N2T3] (presenting case studies in the use of Big Data, which focused on potentially beneficial uses in credit, employment, higher education, and criminal justice).

[18] *See id.* at 22–24 (calling for research, education, training, design, and standards). *But see* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 60 (2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/A7Y9-QUGS] (recommending, inter alia, advancing a Consumer Privacy Bill of Rights, national data breach legislation, and antidiscrimination measures, and amending the Electronic Communications Privacy Act).

[19] *E.g.*, Joel R. Reidenberg, *Yes: Our Experiment with Self-Regulation Has Failed, in Should the U.S. Adopt European-Style Data-Privacy Protections?*, WALL STREET J. (Mar. 10, 2013, 4:00 PM), http://www.wsj.com/articles/SB10001424127887324338604578328393797127094 [https://perma.cc/A59X-RZNH].

[20] *See* HITPC PRIVACY & SEC. WORKGROUP, HEALTH BIG DATA RECOMMENDATIONS 15–20 (2015), https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf [https://perma.cc/9ZEZ-TJ2M] (recommending, inter alia, amendments to HIPAA privacy and security rules).

[21] *Cf.* Rucke, *supra* note 16.

[22] Dibya Sarkar, *Consumer Control, Consent on Privacy Not Outdated, Ramirez Tells TPI*, COMM. DAILY (Aug. 23, 2016), http://www.communicationsdaily.com/article/print?id=501993.

[23] THE NETWORKING & INFO. TECH. RESEARCH & DEV. PROGRAM, THE FEDERAL BIG DATA RESEARCH AND DEVELOPMENT STRATEGIC PLAN 27 (2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/NSTC/bigdatardstrategicplan-nitrd_final-051916.pdf [https://perma.cc/QT8K-XGP9].

done at this point in time to assure individuals that their personal privacy is protected. According to FTC Chairwoman Edith Ramirez, "[t]here is a risk we won't really be able to innovate, we won't really be able to make full use of big data . . . unless we really do make sure that consumers feel that they have control."[24] The most certain way to create the feeling that consumers have control is to actually confer control through privacy-by-design, algorithmic transparency, and privacy-sensitive corporate policies and government regulations well-communicated to a digitally educated public. To "unleash the full potential of big data," according to Ramirez, "the principles of transparency and choice that undergird privacy laws around the world — as well as the best practices the FTC advocates — [must] continue to play an important role in protecting consumer privacy."[25] Participation in this debate, and encouragement of the development of novel and creative methods of returning privacy controls to the individual, can be a powerful way to engage ethically within the current framework.

V. CONCLUSION

While individuals have a moral responsibility to protect their own privacy, Big Data represents a challenge that points to the need for collective and political approaches to self-protection rather than solely individual, atomistic approaches. Fortunately, although business and government are "all in" with Big Data, privacy concerns are getting some of the attention they deserve from policymakers and researchers. As we push business and government to address the complex threat to privacy posed by Big Data, we can also look forward to ways Big Data may improve the experience of privacy and private life.

[24] Sarkar, *supra* note 22 (quoting Ramirez's response to a question from N.Y.U. economist Larry White).

[25] *Id.* (quoting Ramirez).