66 STAN. L. REV. ONLINE 47
September 3, 2013

BUYING AND SELLING PRIVACY: BIG DATA'S DIFFERENT BURDENS AND BENEFITS

Joseph W. Jerome*

Big data is transforming individual privacy—and not in equal ways for all. We are increasingly dependent upon technologies, which in turn need our personal information in order to function. This reciprocal relationship has made it incredibly difficult for individuals to make informed decisions about what to keep private. Perhaps more important, the privacy considerations at stake will not be the same for everyone: they will vary depending upon one's socioeconomic status. It is essential for society and particularly policymakers to recognize the different burdens placed on individuals to protect their data.

I. THE VALUE OF PRIVACY

Privacy norms can play an important role defining social and individual life for rich and poor. In his essay on the social foundations of privacy law, the dean of Yale Law School, Robert Post, argued that privacy upholds social "rules of civility" that create "a certain kind of human dignity and autonomy which can exist only within the embrace of community norms."[1] He cautioned that these benefits would be threatened when social and communal relationships were replaced by individual interactions with "large scale surveillance organizations."[2]

Today, privacy has become a commodity that can be bought and sold. While many would view privacy as a constitutional right or even a funda-

* Legal and Policy Fellow, Future of Privacy Forum.

1. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989).

2. *See id.* at 1009 (suggesting that the relationships between individuals and large organizations are "not sufficiently textured or dense to sustain vital rules of civility" and instead emphasize raw efficiency in data collection).

mental human right,[3] our age of big data has reduced privacy to a dollar figure. There have been efforts—both serious and silly—to quantify the value of privacy. Browser add-ons such as Privacyfix try to show users their value to companies,[4] and a recent study suggested that free Internet services offer $2,600 in value to users in exchange for their data.[5] Curiously, this number tracks closely with a claim by Chief Judge Alex Kozinski that he would be willing to pay up to $2,400 per year to protect his family's online privacy.[6] In an interesting Kickstarter campaign, Federico Zannier decided to mine his own data to see how much he was worth. He recorded all of his online activity, including the position of his mouse pointer and a webcam image of where he was looking, along with his GPS location data for $2 a day and raised over $2,700.[7]

"Monetizing privacy" has become something of a holy grail in today's data economy. We have seen efforts to establish social networks where users join for a fee and the rise of reputation vendors that protect users' privacy online, but these services are luxuries. And when it comes to our privacy, price sensitivity often dictates individual privacy choices. Because the "price" an individual assigns to protect a piece of information is very different from the price she assigns to sell that same piece of information, individuals may have a difficult time protecting their privacy.[8] Privacy clearly has financial value, but in the end there are fewer people in a position to pay to secure their privacy than there are individuals willing to sell it for anything it's worth.

A recent study by the European Network and Information Security Agency discovered that most consumers will buy from a more privacy-invasive provider if that provider charges a lower price.[9] The study also

---

3. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (suggesting that constitutional guarantees create zones of privacy); Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

4. Joe Mullin, *How Much Do Google and Facebook Profit from Your Data?*, ARS TECHNICA (Oct. 9, 2012, 6:38 AM PDT), http://arstechnica.com/tech-policy/2012/10/how-much-do-google-and-facebook-profit-from-your-data.

5. *Net Benefits: How to Quantify the Gains that the Internet Has Brought to Consumers*, ECONOMIST (Mar. 9, 2013), http://www.economist.com/news/finance-and-economics/21573091-how-quantify-gains-internet-has-brought-consumers-net-benefits.

6. Matt Sledge, *Alex Kozinksi, Federal Judge, Would Pay a Maximum of $2,400 a Year for Privacy*, HUFFINGTON POST (Mar. 4, 2013, 5:51 PM EST), http://www.huffingtonpost.com/2013/03/04/alex-kozinski-privacy_n_2807608.html.

7. Federico Zannier, *A Bite of Me*, KICKSTARTER, http://www.kickstarter.com/projects/1461902402/a-bit-e-of-me (last visited Aug. 29, 2013).

8. *See, e.g.,* Alessandro Acquisti et al., What Is Privacy Worth? 27-28 (2010) (unpublished manuscript), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

9. NICOLA JENTZSCH ET AL., EUR. NETWORK & INFO. SEC. AGENCY, STUDY ON MONETISING PRIVACY: AN ECONOMIC MODEL FOR PRICING PERSONAL INFORMATION 1 (2012), *available at* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport.

noted that when two companies offered a product for the same price, the more privacy-friendly provider won out. This was hailed as evidence that a pro-privacy business model could succeed, but this also anticipates that, all things being equal, one company would choose not to collect as much information as a competitor just to be seen as "privacy friendly." This defeats much of the benefit that a big data economy promises.

II. THE BIG DATA CHALLENGE

The foundations of big data rest on collecting as much raw information as possible before we even begin to understand what insight can be deduced from the data. As a result, long-standing Fair Information Practices like collection limits and purpose limitations are increasingly viewed as anachronistic,[10] and a number of organizations and business associations have called for privacy protections to focus more on how data might be used rather than limit which data can be collected.[11] The conversation has moved away from structural limitations toward how organizations and businesses can build "trust" with users by offering transparency.[12] Another suggestion is to develop business models that will share the benefits of data more directly with individuals. Online data vaults are one potential example, while the Harvard Berkman Center's "Project VRM" proposes to rethink how to empower users to harness their data and control access to it.[13] In the meantime, this change in how we understand individual privacy may be

10. Since their inception three decades ago, the Fair Information Practices, which include principles such as user notice and consent, data integrity, and use limitations, have become the foundation of data protection law. For a thorough discussion and a critique, see Fred H. Cate, *The Failure of the Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 343 (2006).

11. *See, e.g.*, WORLD ECON. F., UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 4 (2013), *available at* http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf. In the lead-up to the National Telecommunications and Information Administration's privacy multistakeholder process, the Telecommunications Industry Association demanded that the group's "focus should be on regulating how personal information is used, rather than how it is collected." Press Release, Telecomms. Indus. Ass'n, Telecommunications Industry Association Says NTIA Privacy Code Should Focus on Data Use, Not Collection Method (July 12, 2012), http://www.tiaonline.org/news-media/press-releases/telecommunications-industry-association-says-ntia-privacy-code-should.

12. Michael Fertik, *Big Data, Privacy, and the Huge Opportunity in the Monetization of Trust*, WORLD ECON. F. BLOG (Jan. 25, 2012, 2:13 AM), http://forumblog.org/2012/01/davos-daily-big-data-privacy-and-the-huge-opportunity-in-the-monetization-of-trust.

13. VRM stands for "Vendor Relationship Management." According to the Harvard Berkman Center, the goal of the project is to "provide customers with both *independence* from vendors and *better ways of engaging* with vendors." *ProjectVRM*, HARV. UNIV. BERKMAN CTR. FOR INTERNET & SOC'Y, http://cyber.law.harvard.edu/projectvrm/Main_Page (last updated Mar. 27, 2013, 07:07 PM). It hopes Project VRM can improve individuals' relationships with not just businesses, but schools, churches, and government agencies. *Id.*

inevitable—it may be beneficial—but we need to be clear about how it will impact average individuals.

A recent piece in the *Harvard Business Review* posits that individuals should only "sell [their] privacy when the value is clear," explaining that "[t]his is where the homework needs to be done. You need to understand the motives of the party you're trading with and what [he] ha[s] to gain. These need to align with your expectations and the degree to which you feel comfortable giving up your privacy."[14] It could be possible to better align the interests of data holders and their customers, processing and monetizing data both for business and individual ends. However, the big challenge presented by big data is that the value may not be clear, the motives let alone the identity of the data collector may be hidden, and individual expectations may be confused. Moreover, even basic reputation-management and data-privacy tools require either users' time or money, which may price out average consumers and the poor.

III. BIG DATA AND CLASS

Ever-increasing data collection and analysis have the potential to exacerbate class disparities. They will improve market efficiency, and market efficiency favors the wealthy, established classes. While the benefits of the data economy will accrue across society, the wealthy, better educated are in a better position to become the type of sophisticated consumer that can take advantage of big data.[15] They possess the excellent credit and ideal consumer profile to ensure that any invasion of their privacy will be to their benefit; thus, they have much less to hide and no reason to fear the intentions of data collectors. And should the well-to-do desire to maintain a sphere of privacy, they will also be in the best position to harness privacy-protection tools and reputation-management services that will cater to their needs. As a practical matter, a monthly privacy-protection fee will be easier for the wealthy to pay as a matter of course. Judge Kozinski may be willing and able to pay $200 a month to protect his privacy, but the average consumer might have little understanding what this surcharge is getting him.

The lower classes are likely to feel the biggest negative impact from big data. Historically, the poor have had little expectation of privacy—castles and high walls were for the elite, after all. Even today, however, the poor are the first to be stripped of fundamental privacy protections. Professor

14. Chris Taylor & Ron Webb, *A Penny for Your Privacy?*, HBR BLOG NETWORK (Oct. 11, 2012, 11:00 AM), http://blogs.hbr.org/cs/2012/10/a_penny_for_your_privacy.html.

15. For a discussion of the "winners and losers" of big data, see Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2021-33 (2013); Omer Tene, *Privacy: For the Rich or for the Poor?*, CONCURRING OPINIONS (July 26, 2012, 2:05 AM), http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html (discussing the argument that the pervasive collection of personal information allows companies "to make the poor subsidize luxury goods for the rich").

Christopher Slobogin has noted what he calls a "poverty exception" to the Fourth Amendment, suggesting that our expectations of privacy have been defined in ways that make the less well-off more susceptible to experience warrantless government intrusions into their privacy and autonomy.[16] Big data worsens this problem. Most of the biggest concerns we have about big data—discrimination, profiling, tracking, exclusion—threaten the self-determination and personal autonomy of the poor more than any other class. Even assuming they can be informed about the value of their privacy, the poor are not in a position to pay for their privacy or to value it over a pricing discount, even if this places them into an ill-favored category.

And big data is all about categorization. Any given individual's data only becomes useful when it is aggregated together to be exploited for good or ill. Data analytics harness vast pools of data in order to develop elaborate mechanisms to categorize and organize. In the end, the worry may not be so much about having information gathered about us, but rather being sorted into the wrong or disfavored bucket.[17] Take the example of an Atlanta man who returned from his honeymoon to find his credit limit slashed from $10,800 to $3,800 simply because he had used his credit card at places where other people were likely to have a poor repayment history.[18]

Once everyone is categorized into granular socioeconomic buckets, we are on our way to a transparent society. Social rules of civility are replaced by information efficiencies. While this dynamic may produce a number of very significant societal and communal benefits, these benefits will not fall evenly on all people. As Helen Nissenbaum has explained, "the needs of wealthy government actors and business enterprises are far more salient drivers of their information offerings, resulting in a playing field that is far from even."[19] Big data could effectuate a democratization of information but, generally, information is a more potent tool in the hands of the powerful.

Thus, categorization and classification threaten to place a privacy squeeze on the middle class as well as the poor. Increasingly large swaths of people have little recourse or ability to manage how their data is used. Encouraging people to contemplate how their information can be used—and how best to protect their privacy—is a positive step, but a public educa-

---

16. Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 392, 406 (2003).

17. *See* Tene, *supra* note 15.

18. *See* Lori Andrews, *Facebook Is Using You*, N.Y. TIMES (Feb. 4, 2012), http://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html. Tech analyst Alistair Croll discusses this example, arguing that big data will become a difficult civil rights issue. Alistair Croll, *Big Data Is Our Generation's Civil Rights Issue, and We Don't Know It: What the Data Is Must Be Linked to How It Can Be Used,* O'REILLY RADAR (Aug. 2, 2012), http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html.

19. HELEN NISSENBAUM, PRIVACY IN CONTEXT 211 (2010).

tion campaign, while laudable, may be unrealistic. Social networks, cellular phones, and credit cards—the lifeblood of the big data economy—are necessities of modern life, and assuming it was either realistic or beneficial to get average people to unplug, an overworked, economically insecure middle class does not have the time or energy to prioritize what is left of their privacy.

At present, the alternative to monetizing privacy is to offer individuals the right to make money off their information. Michael Fertik, who runs the online privacy management site, Reputation.com, sees a bright future in allowing companies to "unlock huge value in collaboration with their end users" by monetizing "the latent value of their data."[20] Startups like Personal have tried to set themselves up as individually tailored information warehouses where people can mete out their information to businesses in exchange for discounts.[21] These are projects worth pursuing, but the degree of trust and alignment between corporate and individual interests they will require are significant. Still, it is unlikely we can ever develop a one-to-one data exchange. Federico Zannier sold his personal data at a rate of $2 per day to anyone who would take it as an experiment, but average individuals will likely never be in a position to truly get their money's worth from their personal data. Bits of personal information sell for a fraction of a penny,[22] and no one's individual profile is worth anything until it is collected and aggregated with the profiles of similar socioeconomic categories.

CONCLUSION

While data protection and privacy entrepreneurship should be encouraged, individuals should not have to pay up to protect their privacy or receive coupons as compensation. If we intend for our economic and legal frameworks to shift from data collection to use, it is essential to begin the conversation about what sort of uses we want to take off the table. Certain instances of price discrimination or adverse employment decisions are an easy place to start, but we ought to also focus on how data uses will impact different social classes. Our big data economy needs to be developed such that it promotes not only a sphere of privacy, but also the rules of civility that are essential for social cohesion and broad-based equality.

If the practical challenges facing average people are not considered, big data will push against efforts to promote social equality. Instead, we will be

---

20. Fertik, *supra* note 12.

21. Alexis C. Madrigal, *How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200*, ATLANTIC (Mar. 19, 2012, 3:18 PM ET), http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730.

22. Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html.

categorized and classified every which way, and only the highest high value of those categories will experience the best benefits that data can provide.