BIG DATA: CATALYST FOR A PRIVACY CONVERSATION

JOSEPH JEROME*

INTRODUCTION

In Captain America's latest big screen adventure, his arch-enemy is neither some diabolical super villain nor a swarm of space aliens.[1] Instead, it's big data.[2] "The 21st century is a digital book," the Captain is told.[3] "Your bank records, medical histories, voting patterns, emails, phone calls, your damn SAT scores! [Our] algorithm evaluates people's past to predict their future."[4]

In popular imagination, big data can apparently do everything and anything. Its evangelists would suggest data holds near magical potential to change the world,[5] while skeptics increasingly worry that it poses the biggest civil rights threat of our generation.[6] Even if reality likely falls somewhere in between, there is little question that the advent of big data has altered our conversations about privacy. Privacy has been in tension with technological advances since Louis Brandeis worried that "recent inventions and business methods"—such as the widespread availability of the Kodak camera to consumers—necessitated a "right to be let alone."[7]

Yet the phenomenon of big data, alongside the emerging "Internet of Things,"[8] makes it ever more difficult to be left entirely alone. The ubiquitous

---

* Joseph Jerome is Policy Counsel at the Future of Privacy Forum in Washington D.C. where he focuses on big data and issues around the emerging Internet of Things. Previously, he served as National Law Fellow at the American Constitution Society, where he organized programming on topics involving civil liberties and national security.

1. Josh Bell, *What Captain America Has to Say About the NSA,* FREE FUTURE: PROTECTING CIVIL LIBERTIES IN THE DIGITAL AGE (Apr. 18, 2014, 10:41 AM), https://www.aclu.org/blog/national-security-technology-and-liberty/what-captain-america-has-say-about-nsa.

2. *Id.*

3. *Id.*

4. *Id.*

5. *See* RICK SMOLAN, HUMAN FACE OF BIG DATA (2012). For additional examples of how big data can specifically be used to empower vulnerable populations, see FUTURE OF PRIVACY FORUM, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS (2014), *available at* http://www.futureofprivacy.org/wp-content/uploads/Big-Data-A-Tool-for-Fighting-Discrimination-and-Empowering-Groups-Report1.pdf.

6. *See, e.g.*, ROBINSON + YU, CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE (2014), http://bigdata.fairness.io; *Civil Rights Principles for Era of Big Data*, THE LEADERSHIP CONFERENCE (2014), http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html [hereinafter *Civil Rights Principles*]; Alistair Croll, *Big Data Is Our Generation's Civil Rights Issue, and We Don't Know It*, SOLVE FOR INTERESTING (July 31, 2012), http://solveforinteresting.com/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it/.

7. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 195 (1890).

8. Michael Chui et al., *The Internet of Things*, MCKINSEY Q. (Mar. 2010), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things; Bill

collection and unparalleled use of personal information is breaking down some of society's most common conceptions of privacy.[9] Law and policy appear on the verge of redefining how they understand privacy, and data collectors and privacy advocates are trying to present a path forward. This Article discusses the rise of big data and the role of privacy in both the Fourth Amendment and consumer contexts. It explores how the dominant conceptions of privacy as secrecy and as control are increasingly untenable, leading to calls to focus on data use or respect the context of collection. It argues that the future of privacy will have to be built upon a foundation of trust—between individuals and the technologies that will be watching and listening.

I. THE RISE OF BIG DATA

"Big data" has only recently gone mainstream.[10] Prior to 2012, big data was a buzzword used by engineers and scientists to describe advances in digital communications, computation, and data storage.[11] While some computer scientists remain skeptical of the term,[12] big data has commonly come to represent the drastic increase in the volume, variety, and velocity of data that can be analyzed.[13] Whatever the technical definition of the term, the idea of big data has become something more.

A. What Is Big Data?

danah boyd and Kate Crawford suggest that big data is a "cultural, technological, and scholarly phenomenon" with its own mythology about the untold value of data.[14] Acting almost as heralds of big data's potential, Viktor Mayer-Schönberger and Kenneth Cukier tout the transformation of our entire world into "oceans of data that can be explored" and that can provide us with a new perspective on reality.[15] The size and scope of the data now available

---

Wasik, *Welcome to the Programmable World*, WIRED (May 14, 2013), http://www.wired.com/gadgetlab/ 2013/05/internet-of-things/.

9. Helen Lewis, *'Like' It or Not, Privacy Has Changed in the Facebook Age*, GUARDIAN (Mar. 12, 2013, 4:32 PM), http://www.theguardian.com/commentisfree/2013/mar/12/privacy-facebook-lesbians-relax-online.

10. *Big Data*, GOOGLE TRENDS, http://www.google.com/trends/explore#q=big%20data&cmpt=q (showing interest in the term exploding since 2011).

11. Randal E. Bryant, Randy H. Katz, & Edward D. Lazowska, *Big-Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science, and Society,* COMPUTING COMMUNITY CONSORTIUM, (Dec. 22, 2008), http://www.cra.org/ccc/files/docs/init/Big_Data.pdf.

12. *See* Cesar A. Hidalgo, *Saving Big Data From Big Mouths,* SCIENTIFIC AMERICAN (Apr. 29, 2014), http://www.scientificamerican.com/article/saving-big-data-from-big-mouths/.

13. *The Big Data Conundrum: How to Define It?*, MIT TECH. REV. (Oct. 3, 2013), http://www.technologyreview.com/view/519851/the-big-data-conundrum-how-to-define-it/.

14. danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon,* 15 INFO., COMM., & SOC'Y 662, 663 (2012).

15. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT

promises new insights and new forms of value that will fundamentally change how we interact with one another, the pair argue.[16]

Yet these bold expectations also mean that big data has become something of an amorphous concept, meaning different things to different audiences in different contexts.[17] A better takeaway is to understand big data as shorthand for the broader "datafication" of society.[18] While data analytics crunch the numbers, datafication is being fueled by another buzzword: the emerging "Internet of Things."[19] The Internet of Things is commonly understood to describe the growing network of devices that are linked together through wired and wireless communications technologies embedded in physical devices, from the average smartphone to intelligent thermostats[20] and pills that can actually monitor a patient's digestive tract.[21] By 2015, twenty-five billion devices are projected to be connected to the Internet; this number could double to fifty billion devices by the end of the decade.[22] Simply going about our everyday lives creates a vast trail of "digital exhaust" that can reveal much about us.[23]

The story of our lives now exists in digital form, yet individuals may be only passively aware of what story their data tells. Recent debates over the value of metadata illustrate this point.[24] In the immediate aftermath of revelations of the National Security Agency's (NSA) surveillance programs, government officials stressed that the NSA's action did "not include the content of any communications"[25] and was limited to "just metadata,"[26] largely implying that

---

WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 97 (2013).

16. *Id.* at 6-7.

17. *What Is Big Data?*, DATASCIENCE@BERKELEY (Sept. 3, 2014), http://datascience.berkeley.edu/what-is-big-data/; Alan Charles Raul, *Don't Throw the Big Data Out with the Bathwater*, POLITICO MAG. (April 29, 2014), http://www.politico.com/magazine/story/2014/04/dont-throw-the-big-data-out-with-the-bath-water-106168.html#.U-oyYPeYamQ.

18. Jeff Bertolucci, *Big Data's New Buzzword: Datafication*, INFO. WEEK (Feb. 25, 2013, 11:13 AM), http://www.informationweek.com/big-data/big-data-analytics/big-datas-new-buzzword-datafication/d/d-id/1108797?.

19. Chui, *supra* note 8; *see also* Wasik, *supra* note 8.

20. NEST LABS, https://nest.com/ (last visited Sept. 1, 2014).

21. Nick Bilton, *Disruptions: Medicine That Monitors You,* N.Y. TIMES (Jun. 23 2013, 11:00 AM), http://bits.blogs.nytimes.com/2013/06/23/disruptions-medicine-that-monitors-you/.

22. DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

23. James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY & CO. (2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

24. *See, e.g.*, Jameel Jaffer & Eric Posner, *Is the N.S.A. Surveillance Threat Real or Imagined?*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined.

25. Press Gaggle, Deputy Principal Press Secretary Josh Earnest and Secretary of Education Arne Duncan, en Route Mooresville, NC (June 6, 2013), *available at* http://www.

looking at mere metadata could hardly present a privacy issue. On some level, this distinction makes sense: individuals are quick to assume that their actual conversations—whether in person, over the phone, or through email messaging—reveal more about themselves than a data trail. But our data trails are, in fact, highly sensitive pieces of information.[27]

Smart grid technologies, for example, are not only a complete evolution in how electricity systems operate,[28] but the sensor data they produce also offer a rich source of behavioral information at a granular level:

> Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used. Combined with other information, such as work location and hours, and whether one has children, one can see that assumptions may be derived from such information.[29]

In a way, our digital exhaust is increasingly defining us as individuals. At the same time, big data is also changing *how* we understand this information. Mayer-Schönberger and Cukier suggest that big data is propelling us toward a world of correlation rather than causation.[30] They highlight the notion that big data brings about the "end of theory," and that with enough information, numbers can

---

whitehouse.gov/the-press-office/2013/06/06/press-gaggle-deputy-principal-press-secretary-josh-earnest-and-secretary.

26. Ed O'Keefe, *Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/.

27. Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POL. (Mar. 12 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/; Jane Mayer, *What's the Matter with Metadata?*, NEW YORKER (June 6, 2013), http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata (suggesting that metadata is "much more intrusive than content").

28. *See generally* EXECUTIVE OFFICE OF THE PRESIDENT, NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID: ENABLING OUR SECURE ENERGY FUTURE (2011), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

29. FUTURE OF PRIVACY FORUM & INFORMATION AND PRIVACY COMMISSIONER, SMART PRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION 10-11 (2009), *available at* http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf.

30. MAYER-SCHÖNBERGER & CUKIER, *supra* note 15, at 61.

literally speak for themselves.[31] For example, they point to the personalization and recommendation engines used by Amazon or Netflix as examples of data systems that only know the "what" and not the "why."[32] Netflix embraced this shift to correlation when it bet that its original programming effort, *House of Cards*, would be a major success.[33] Data suggested that David Fincher movies and films starring Kevin Spacey were especially popular on the service—no one knows why exactly—but these data points were enough for Netflix to commit $100 million to bring the two together.[34]

Unchecked, the insights we can uncover in data can turn into what Mayer-Schönberger and Cukier cleverly term the "dictatorship of data."[35] While the pair use that term to caution against fixating on data such that we fail to appreciate its limitation,[36] it may well refer to large structural shifts in power away from individuals and toward opaque data collectors. Evgeny Morozov provocatively suggests that information-rich societies "have reached a point where they want to try to solve public problems without having to explain or justify themselves to citizens."[37]

Many of the insights derived from data can be used for good or for ill, but that is true of any piece of information. The larger worry is that these insights are being uncovered at great expense to individual autonomy. The dictatorship of data arises as we are now faced with uses of data that produce accurate, efficient, or otherwise beneficial results but are still somehow unfair.[38]

B. Big Data's Big Worries

Big data has often been identified as one of the biggest public policy challenges of our time.[39] Recognizing this, in January 2014, President Obama

---

31. *Id.*

32. *Id*. at 52.

33. *House of Cards*, NETFLIX.COM, www.netflix.com/WiMovie/70178217?locale=en-us (last visited Sept. 1, 2014).

34. David Carr, *Giving Viewers What They Want*, N.Y. TIMES, Feb. 24, 2013, http://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html?pagewanted=all; Andrew Leonard, *How Netflix is Turning Viewers into Puppets*, SALON (Feb. 1, 2013), http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/.

35. MAYER-SCHÖNBERGER & CUKIER, *supra* note 15, at 151.

36. *Id.*

37. Evygeny Morozov, *The Real Privacy Problem*, MIT TECH. REV. (Oct. 22, 2013), http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/.

38. *See* Chris Calabrese, Legislative Director ACLU, Panel Discussion on Civil Rights and Big Data (Mar. 14, 2014), *available at* http://newamerica.net/events/2014/civil_rights_and_big_data.

39. Jules Polonetsky et al., *How To Solve the President's Big Data Challenge*, IAPP PRIVACY PERSPECTIVES (Jan. 31, 2014), https://www.privacyassociation.org/privacy_perspectives/post/how_to_solve_the_presidents_big_data_challenge.

began a comprehensive review of how big data is impacting society.[40] The ensuing report has been an important conversation starter; a significant finding of the administration's effort is that big data has the potential to undermine traditional protections that govern how personal information is used in housing, credit, employment, health, education, and the marketplace.[41] Moving forward, policy makers may need to weigh compelling benefits to national security, public health and safety, and sustainable development against new risks to personal autonomy from high-tech profiling and discrimination, increasingly-automated decision making, inaccuracies and opacity in data analysis, and strains in traditional legal protections.[42]

Worries about big data come in many different flavors, but they all largely derive from the ability of data analysis to better discriminate among individuals. Big data is fundamentally about categorization and segmentation.[43] Data analytics harness vast pools of data in order to develop elaborate mechanisms to more efficiently organize categories of information.[44] The challenge, however, is determining where value-added personalization and segmentation end and harmful discrimination begins.[45]

1. Better Price Discrimination.—Improvements in differential pricing schemes—or price discrimination—are often used as an example of how data analytics can harm consumers.[46] Price discrimination describes situations where one consumer is charged a different price for the exact same good based upon some variation in the customer's willingness to pay.[47] Differential pricing is not a new concept, and in fact, it happens every day. Airlines have long been considered the "world's best price discriminators."[48] The cost of a flight is often carefully tied to where a passenger is flying *and* the type of people they are flying with.[49] Price discrimination makes basic economic sense, and it need not

---

40. *See generally* EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

41. *Id.* at iii.

42. *Civil Rights Principles*, *supra* note 6.

43. Howard Fienberg, *Can Big Data and Privacy Coexist?,* MARKETING RESEARCH ASSOCIATION (Sept. 13, 2013), http://www.marketingresearch.org/news/2013/09/13/can-big-data-and-privacy-coexist.

44. Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HBR BLOG NETWORK (Jan. 29, 2014, 8:00 AM), http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/.

45. *Id.*

46. *See* Fed. Trade Comm'n, *Spring Privacy Series: Alternative Scoring Products* (Mar. 19, 2014), http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

47. *Id.*

48. Scott McCartney, *The Most Expensive Airports to Fly To*, WALL ST. J. (May 22, 2014), online.wsj.com/news/articles/SB10001424052702303980004579576012567760336.

49. *Id.* As a result, it currently costs more for U.S. travelers to fly to Europe than vice versa

necessarily be a bad thing.

What has changed in the age of big data, however, is the granularity at which firms can engage in price discrimination. Historically, prices could vary based upon the quantity of a good purchased, such as bulk order discounts, or prices could be based upon broad consumer categorizations, such as higher car insurance rates for young drivers.[50] With big data, we are moving toward a world where it is much easier to identify individual characteristics in such a way that every individual is charged based on their exact willingness to pay.[51] This type of price discrimination used to be incredibly challenging, if impossible.

Access to information in this fashion creates winners and losers.[52] For much of the twentieth century, consumers were in many ways the ultimate winners: pricing was largely democratized as consumers were offered products and services on identical terms.[53] The rise of the Internet initially provided consumers with an even greater advantage through the promise of quick comparison shopping, but the subsequent proliferation of tracking technologies and data sharing has made archaic any suggestion that the Internet is merely an impersonal tool for use by consumers.[54] While some recognize this information exchange as a basic improvement in market efficiency,[55] some consumers will necessarily lose in the process. Sophisticated consumers may be in a better position to take advantage of these shifts, but having access to so much granular data on individuals will ensure some are sorted into disfavored categories.[56] The larger worry is that big data can—and is being used to—exploit or manipulate certain classes of consumers.[57]

Moreover, individuals are both unaware of what is happening and how it is

---

because the U.S. has a stronger economy and quite literally can afford higher prices.

50. Adam Ozimek, *Will Big Data Bring More Price Discrimination?* FORBES (Sept. 1, 2013, 10:48 AM), http://www.forbes.com/sites/modeledbehavior/2013/09/01/will-big-data-bring-more-price-discrimination/.

51. *Id*.; *see also* Lior Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2027-43 (2013); Fed. Trade Comm'n, *supra* note 46.

52. *See generally* Strahilevitz, *supra* note 51.

53. Fed. Trade Comm'n, *supra* note 46 (Joseph Turow describing how pricing has evolved over time); Strahilevitz, *supra* note 51, at 2027.

54. Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J., Dec. 24, 2012, http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534.

55. THOMAS M. LENARD & PAUL H. RUBIN, THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS, 21-22 (2013), *available at* http://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf.

56. *See, e.g.*, Joseph Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47 (2013); Fed Trade Comm'n, *supra* note 46. (discussing how easily and opaquely companies can make it harder for consumers to get better deals, Ashkan Soltani posed the basic question: "[W]ho wants to be included in [a] higher priced consumer category?").

57. Fed. Trade Comm'n, *supra* note 46.

happening.[58] While recognizing the legitimate value of price discrimination, the White House's Big Data Review cautioned that the capacity for data analytics "to segment the population and to stratify consumer experiences so seamlessly as to be almost undetectable demands greater review."[59]

2. Filter Bubbles & Surveillance.—Because so much of this data collection and analysis happens passively and without any active participation by individuals, individuals are caught behind a sort of data-driven one-way mirror. The resulting concern is that big data allows large data collectors, be they industry or government, to know more about an individual than that individual knows about himself or herself.

Even if organizations have the best of intentions, the knowledge gained from analysis of big data can quickly lead to over-personalization. Profiling algorithms can create "echo chambers" that create feedback loops that reaffirm and narrow an individual's thoughts and beliefs.[60] Eli Pariser first explained how "filter bubbles" could occur by pointing to Google's increasing efforts to improve and personalize searches: Pariser noted that one friend who entered "Egypt" into Google search saw information about the then-occurring Egyptian revolution while another received a list of travel agents and top tourist attractions.[61]

Over time, this has not only raised large questions about individual autonomy, but it also may pose a serious risk to core democratic values. By automatically sorting us into ideological or culturally segregated enclaves, there are worries that filter bubbles may lead to increased polarization.[62] As Joseph Turow explains, "the industrial logic behind the[se] activities makes clear that the

---

58. *FRONTLINE: United States of Secrets* (PBS television broadcast) (transcript *available at* http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/transcript-61/) (Barton Gellman: "Corporate America and law enforcement and national security state know so much about us. And we know so little about them. We know so little about what they're doing, how they're doing it.")

59. EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 47 (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

60. *See* Cynthia Dwork & Deirdre Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35 (2013); *see generally* JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH (2011); *see also* CASS R. SUNSTEIN, REPUBLIC.COM.2.0 (2009).

61. *See, e.g.*, ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK (2012). More recently, Christian Rudder, one of the founders of OkCupid, suggested that Google's search autocomplete function was "the site acting not as Big Brother but as older Brother, giving you mental cigarettes" that could reinforce and perpetuate stereotypes or inaccuracies based on collective misinformation. CHRISTIAN RUDDER, DATACLYSM: WHO WE ARE (WHEN WE THINK NO ONE'S LOOKING) 132 (2014).

62. *But see* Farhad Manjoo, *The End of the Echo Chamber*, SLATE (Jan. 17, 2012, 11:00 AM), http://www.slate.com/articles/technology/technology/2012/01/online_echo_chambers_a_study_of_250_million_facebook_users_reveals_the_web_isn_t_as_polarized_as_we_thought_html (discussing Facebook study that suggests link-sharing is not as polarizing as assumed).

emerging marketplace will be far more an inciter of angst over social difference than a celebration of the 'American salad bowl.'"[63]

While filter bubbles present one end result of ubiquitous data collection and analysis, surveillance may be equally likely to shape individual behavior. Surveillance, like filter bubbles, can encourage like-mindedness and conformity, as well as anxiety and a general chilling effect on civil discourse.[64] For example, pervasive web tracking presents the possibility that people may avoid certain searches or sources of information out of fear that accessing that information would reveal interests, medical conditions, or other characteristics they would prefer be kept hidden.[65] Combined with a lack of transparency about how this information is being used, individuals may feel anxiety over consequential decisions about them being made opaquely, inducing a sense of powerlessness.[66]

A survey in November 2013 revealed just how much revelations about the extent of NSA surveillance had begun to chill speech.[67] Twenty-four percent of writers surveyed admitted they had engaged in self-censorship in email and phone conversations, and sixteen percent had avoided conducting Internet searches of visiting websites that could be considered controversial or suspicious.[68] Examples of controversial subjects included national security, mass incarceration, drug policy, pornography, and even general criticism of the U. S. government.[69]

3. A New Civil Rights Movement.—Recently, critics, including some of the United States' leading civil rights organizations, have argued that big data could be the "civil rights" issue of this generation.[70] The fear is that data determinism—or the dictatorship of data—could work to undermine equal opportunity and equal justice through either hidden or new forms of discrimination.[71] Big data could achieve these harms by contributing to currently illegal practices, allowing otherwise unlawful activity to go undetected due to a lack of transparency or access surrounding data analysis.[72] Alternatively, big data

---

63. JOSEPH TUROW, NICHE ENVY: MARKETING DISCRIMINATION IN THE DIGITAL AGE 2 (2006).

64. Chris Chambers, *Indiscriminate Surveillance Fosters Distrust, Conformity, and Mediocrity: Research* RAWSTORY.COM (Aug. 26, 2013), http://www.rawstory.com/rs/2013/08/26/indiscriminate-surveillance-fosters-distrust-conformity-and-mediocrity-research/.

65. FELIX WU, BIG DATA THREATS 2 (2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Wu-Big-Data-Threats.pdf.

66. *Id.*; *see also* Matt Stroud, *The Minority Report: Chicago's New Police Computer Predicts Crimes, But Is It Racist?*, VERGE (Feb. 19, 2014, 9:31 AM), http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist.

67. PEN AMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 6 (2013), *available at* http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

68. *Id.*

69. *Id.*

70. Croll, *supra* note 6; *Civil Rights Principles*, *supra* note 6.

71. *Civil Rights Principles*, *supra* note 6.

72. Pam Dixon, *On Making Consumer Scoring More Fair and Transparent*, IAPP PRIVACY

may introduce societal biases that may impact protected classes or otherwise vulnerable populations disproportionately or unfairly.[73]

Some have argued that more data could actually mitigate arbitrariness or "gut instinct" in decision-making,[74] but even if algorithms produce the correct decision, that does not mean the decision is necessarily fair. Take the example of an Atlanta man who returned from his honeymoon to find his credit limit slashed from $10,800 to $3,800 because he had used his credit card at locations where *others* were likely to have a poor repayment history.[75] Is this a sensible decision for a credit card company to take, or does it remain somehow fundamentally unfair?

Many of our key anti-discrimination laws work to address classifications or decisions that society has deemed either irrelevant or illegitimate. The Equal Credit Opportunity Act, for example, explicitly forbids creditors from asking about a candidate's marital status or plans to have children.[76] An even better example is the Genetic Information Nondiscrimination Act of 2008, which prohibits employers from using an applicant's or an employee's genetic information as the basis of an employment decision, and it also limits the ability of health insurance organizations to deny coverage based solely on a genetic predisposition to develop a disease.[77] As a matter of public policy, our laws make a point of excluding genetic information that could no doubt lead to more accurate decision-making.

Moreover, big data can introduce new forms of discrimination due to bias errors or incomplete data, and it may make intentional discrimination harder to detect.[78] As Kate Crawford explains, "not all data is created or even collected equally" and "there are 'signal problems' in big-data sets—dark zones or shadows where some citizens and communities are overlooked or underrepresented."[79]

PERSPECTIVES (Mar.19, 2014), https://www.privacyassociation.org/privacy_perspectives/post/on_making_consumer_scoring_more_fair_and_transparent.

73. *See* Kate Crawford, *The Hidden Biases in Big Data*, HBR BLOG NETWORK (Apr.1, 2013), http://blogs.hbr.org/2013/04/the-hidden-biases-in-big-data/.

74. LENARD & RUBIN, *supra* note 55, at 7.

75. *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.

76. 15 U.S.C. § 1691 (2006).

77. Pub. L. No. 110-233, § 122 Stat. 881 (2008).

78. Solon Barocas & Andrew Selbst, Big Data's Disparate Impact 3 (2014) (unpublished manuscript) (on file with author).

79. Kate Crawford, *Think Again: Big Data*, FP.COM (May 9, 2013), www.foreignpolicy.com/articles/2013/05/09/think_again_big_data; *see also* Crawford, *supra* note 73 (Crawford discusses the now infamous example of Boston's StreetBump app, which allowed residents to report potholes through a mobile app. The city quickly realized that wealthy residents were far more likely to own smartphones and cars and, thus, the map of potential potholes reflected only where the wealthy were most likely to travel.); *see also* Jonas Lerman, *Big Data and Its Exclusions*, 66 STAN. L. REV. ONLINE 55 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/big-data-and-its-exclusions (Lerman argues that big data could end up excluding some

Discriminatory data begets discriminatory decisions.

The privacy challenge is that many of these risks are abstract or inchoate. They are not easily mapped to recognizable harms or are difficult to link to accepted privacy risks. To what degree they even represent real challenges to society—or are mere "boogeyman scenarios" or "hypothetical horribles"[80]—remains an open question. Yet it is against this backdrop that big data is on a collision course with our traditional privacy frameworks.

II. THE ROLE OF PRIVACY

Like big data, privacy also suffers from a multiplicity of meaning. Thomas McCarthy suggested that privacy, like "freedom" or "liberty," has become a powerful rhetorical battle cry within a plethora of unrelated contexts.[81] As a result, privacy has become entangled with policy debates ranging from education reform[82] to the future of robotics.[83] Scholars have wrestled with how to understand and define privacy, and ultimately to describe its value.[84] For example, Daniel Solove has suggested that privacy works as a set of protections against a variety of distinct but related problems.[85] He proposes a comprehensive privacy taxonomy that focuses on activities that invade privacy, but his notion that privacy is multifaceted also helps to explain why different privacy theories are deployed within different contexts. Two of the broadest and most common conceptions of privacy consider privacy to be about either (1) secrecy or (2)

---

members of society, as a result.).

80. Adam Thierer, *Planning for Hypothetical Horribles in Tech Policy Debates*, TECH. LIBERATION FRONT (Aug. 6, 2013), http://techliberation.com/2013/08/06/planning-for-hypothetical-horribles-in-tech-policy-debates/.

81. J. Thomas McCarthy, THE RIGHTS OF PUBLICITY AND PRIVACY 1-3, 5-65 (1992) (discussing section 1.1(B)(1) and section 5.7(D)).

82. Benjamin Herold, *inBloom to Shut Down Amid Growing Data-Privacy Concerns*, EDWEEK (Apr. 21, 2014, 10:33 AM), http://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html.

83. Mark Stephen Meadows, *Is Surveillance the New Business Model for Consumer Robotics?,* ROBOHUB (May 6, 2014), http://robohub.org/is-surveillance-the-new-business-model-for-consumer-robotics/.

84. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE, PART II (2009) (giving an overview of competing theories); *see also* DANIEL SOLOVE, UNDERSTANDING PRIVACY 1-12 (2008); *see also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (looking at how privacy intersects different legal categories).

85. SOLOVE, *supra* note 84, at 171.

control.[86] Privacy-as-secrecy is often invoked in debates about the relationship between government prerogatives and individual privacy, while privacy-as-control predominates within the context of consumer privacy.[87] Both theories are increasingly challenged by technology—and big data in particular.

A. Fourth Amendment Protections: Privacy as Secrecy

Traditionally, privacy was viewed as being roughly analogous to secrecy.[88] Privacy-as-secrecy has been a particularly dominant theme in the U.S. Supreme Court's Fourth Amendment search jurisprudence since *Katz v. United States*.[89] Decided in 1967, *Katz* emerged in an environment where new, more sophisticated surveillance technologies forced the Court to re-conceive how Fourth Amendment protections work.[90] In *Katz*, FBI agents had attached a bug to the outside of a public telephone booth in order to monitor the defendant's communications without first obtaining a warrant.[91] Ignoring a lack of any physical trespass—a factor that had previously dominated the Court's thinking[92]—the Court clearly had secrecy on its mind when it held that what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[93]

Katz is most famous, however, for producing Justice Harlan's concurrence discussing whether or not individuals may have a "reasonable expectation of privacy."[94] The test for determining whether one has a reasonable expectation of

---

86. *See generally* Bruce Schneier, *Privacy and Control*, SCHNEIER ON SECURITY (Apr. 6, 2010, 7:47 AM), https://www.schneier.com/blog/archives/2010/04/privacy_and_con.html ("To the older generation, privacy is about secrecy. And, as the Supreme Court said, once something is no longer secret, it's no longer private. But that's not how privacy works, and it's not how the younger generation thinks about it. Privacy is about control.").

87. David E. Sanger, *In Surveillance Debate, White House Turns Its Focus to Silicon Valley,* N.Y. TIMES (May 2, 2014), http://www.nytimes.com/2014/05/03/us/politics/white-house-shifts-surveillance-debate-to-private-sector.html?_r=0.

88. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978) (exploring a concept of privacy as concealment of facts and communications); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42-44 (2004) (discussing a "secrecy paradigm").

89. Katz v. United States, 389 U.S. 347 (1967).

90. *See* Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1305 (2002).

91. *Katz*, 389 U.S., at 348-49.

92. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, SUP. CT. REV. 86-95 (2013).

93. *Id.*

94. In time, Justice Harlan's concurring opinion effectively became the holding of the *Katz* opinion. *See, e.g.*, Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 6-7 (2009) ((citing Minnesota v. Carter, 525 U.S. 83, 97 (1998)) (suggesting the *Katz* test "has come to mean the test enunciated by Justice Harlan's separate concurrence in Katz")); *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (expressly adopting

privacy claims to be an objective assessment of what society reasonably regards as private.[95] Yet this test involves a degree of circularity: judicial rulings are to be guided by societal expectations, but societal expectations are necessarily shaped by judicial rulings. As Justice Alito recently noted, the *Katz* test regularly causes judges to "confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[96] In fact, as Christopher Slobogin has shown, the U.S. Supreme Court's conclusions about society's privacy expectations are often misguided, ignoring both positive law governing ordinary citizens and public opinion generally.[97] As a result, in practice, the *Katz* test often serves as a one-way ratchet against privacy.

This is particularly true when privacy is exclusively understood as being related to secrecy. The *Katz* test does this by insisting that anything a person "knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[98] As a result, the law treats *any* partial exposure—and any *risk* of exposure—of private matters as functionally exposing that concern to the entire world, relinquishing any privacy rights an individual may have as a result.[99] For example, even though society generally frowns upon sifting through a neighbor's trash, the U.S. Supreme Court has determined trash is "knowingly exposed" to the public and therefore, no reasonable expectation of privacy can be claimed should the government wish to search it.[100]

The logical result of treating privacy as secrecy is the much maligned "third-party doctrine," which governs the collection of information from third parties in criminal investigations.[101] The Court has repeatedly held that individuals have

---

Justice Harlan's "reasonable expectation of privacy" formula as the rule of *Katz*).

95. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting); *see also* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 560 (1990) (calling the subjective prong "useless"); Simmons, *supra* note 90, at 1312 (calling any subjective element "meaningless").

96. United States v. Jones, 132 S. Ct. 945, 962 (2012); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001).

97. *See generally* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007).

98. Katz v. United States, 389 U.S. 347, 351 (1967).

99. *See, e.g.*, Sherry F. Colb, *The Supreme Court Decides the GPS Case*, *United States v. Jones, and the Fourth Amendment Evolves*, JUSTIA VERDICT (Feb. 15, 2012), http://verdict.justia.com/2012/02/15/the-supreme-court-decides-the-gps-case-united-states-v-jones-and-the-fourth-amendment-evolves-2. For a more extensive discussion of the analytical missteps the Court has made, see also Sherry F. Colb, *What Is A Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of A Remedy*, 55 STAN. L. REV. 119, 122 (2002).

100. *Compare* California v. Greenwood, 486 U.S. 35 (1988), *with id.* at 45 ((Brennan, J., dissenting) ("Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior.")).

101. *See* Orin Kerr, *In Defense of the Third-Party Doctrine*, 107 MICH. L. REV. 561, (2009), *available at* http://www.michiganlawreview.org/assets/pdfs/107/4/kerr.pdf.

no reasonable expectation of privacy in information provided to a third party.[102] In *United States v. Miller*, the Court found that individuals had no expectation of privacy in their bank records because "a depositor takes the risk" that their information could be shared—"even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[103]

Miller was cited again in *Smith v. Maryland*, which dealt with phone records captured and recorded by pen register devices.[104] According to the U.S. Supreme Court, when the defendant used his phone, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[105] Crucially, the third-party doctrine applied even where the telephone company had entirely automated its record process.[106] This suggests that there is no legal difference between the disclosure of information to a human being or an automated system, which with the development of the Internet, effectively eliminated any possibility of Fourth Amendment protection for online data.[107]

As we now know, *Smith v. Maryland* provided key constitutional support for the NSA's controversial bulk metadata collection program under Section 215 of the Patriot Act.[108] This, despite the fact the U.S. Supreme Court has cautioned that any "dragnet-type law enforcement practices" like "twenty-four hour surveillance of any citizen," might receive heightened scrutiny under the Fourth Amendment.[109] The series of disclosures by Edward Snowden in 2013 have produced many legal challenges, and in *Klayman v. Obama*, the District Court granted a preliminary injunction against a NSA surveillance program on the grounds that it was impossible to "navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[110]

Technology often appears to challenge the judiciary as a whole—and the U.S. Supreme Court in particular.[111] When privacy and technology collide, the result is often more confusion than anything. A perfect example of this was the recent unanimous finding in *United States v. Jones* that sustained warrantless use of a

---

102. *See, e.g.,* United States v. Miller, 425 U.S.435 (1976).

103. *Id.* at 443.

104. Smith v. Maryland, 442 U.S. 735 (1979).

105. *Id*. at 744.

106. *Id*. at 744-45.

107. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 600 (2011).

108. *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted]*, http://www.fas.org/irp/agency/doj/fisa/fisc-082913.pdf.

109. United States v. Knotts, 460 U.S. 276, 284 (1983).

110. Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013).

111. Lawrence Hurley, *In U.S., When High-Tech Meets High Court, High Jinks Ensue*, REUTERS (May 9, 2014, 1:12 PM), http://www.reuters.com/article/2014/05/09/us-usa-court-tech-idUSBREA480N420140509.

GPS-tracking device violated the Fourth Amendment.[112] While the Court was unanimous in finding a Fourth Amendment violation, the justices splintered in explaining *why* a violation had occurred.[113] In a concurring opinion authored by Justice Alito, four justices relied on the *Katz* test to hold that any long-term monitoring violated the defendant's reasonable expectation of privacy.[114] Led by Justice Scalia, four justices embraced a trespass rationale, which Justice Sotomayor joined to create a five-vote majority while also agreeing with Justice Alito's analysis.[115]

The *Jones* decision was considered "puzzling" and "confusing," leaving many of the case's privacy implications unanswered.[116] Justice Alito ominously conceded that a "diminution of privacy" may be "inevitable," and suggested further that society may find it "worthwhile" to trade convenience and security "at the expense of privacy."[117]

Alone among her colleagues, Justice Sotomayor recognized the looming threat of pervasive government surveillance.[118] New technologies, she observed, permit the government to collect more and more data and cost less and less to implement.[119] The technological invasion of citizens' privacy was clearly "susceptible to abuse" and over time could "alter the relationship between citizen and government in a way that is inimical to democratic society."[120] Moreover, she challenged not just the third-party doctrine but the Court's entire understanding of society's reasonable expectation of privacy.[121] Faced with an influx of new surveillance technologies, she argued that it is now time "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed . . . to some member of the public for a limited purpose," suggesting that the courts should "cease[] to treat secrecy as a prerequisite for privacy."[122]

---

112. United States v. Jones, 132 S. Ct. 945, 954 (2012).

113. *Id.*

114. *Id.* at 958.

115. *Id.* at 955.

116. *See* Orin Kerr, *Why United States v. Jones is Subject to So Many Different Interpretations*, VOLOKH CONSPIRACY (Jan. 30, 2012), http://www.volokh.com/2012/01/30/why-united-states-v-jones-is-subject-to-so-many-different-interpretations/; *see also* Tom Goldstein, *Why Jones is Still Less of a Pro-Privacy Decision Than Most Thought*, SCOTUSBLOG (Jan. 30, 2012), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought/ *(conclusion slightly revised Jan. 31)*.

117. *Jones*, 132 S. Ct. at 962.

118. *Id.* at 956.

119. *See* Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, YALE L.J (Jan. 9, 2014) http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

120. *Jones*, 132 S. Ct. at 956.

121. *Id.*

122. *Id.* at 957.

B. Consumer Privacy: Privacy as Control

Alan Westin famously defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[123] According to Westin, individuals engage in a continuous process of personal adjustment that weighs individual privacy interests against their social desires. While notions about "reasonable expectations of privacy" can occasionally inform consumer privacy issues,[124] consumer privacy is dominated by an understanding of privacy as privacy-as-control.

From "Do Not Call" registries to informed consent requirements under various health and financial privacy laws, privacy is promoted by giving individuals choices about their own information flows. The 2012 White House Consumer Privacy Bill of Rights builds on this.[125] The document places a principle of individual control front and center, before any other consumer right, declaring that "[c]onsumers have a right to exercise control over what personal data companies collect from them *and* how they use it."[126]

Individual control is expressed throughout a number of traditional Fair Information Practice Principles (FIPPs). The FIPPs are the bedrock of modern privacy law.[127] Similar to how technological changes motivated *Katz*,[128] the FIPPs emerged in the early 1970s against a backdrop of government surveillance scandals and rising worries about the use of early automated data systems.[129] They established a framework for both the public and private sectors to implement procedures governing the collection, use, and disclosure of personal information.[130] These principles were incorporated into the Privacy Act of

---

123. *See* Alan Westin, *Privacy and Freedom*, 25 WASH. & LEE L. REV. 166 (1968)

124. *See*, *e.g.*, Christopher Wolf, *Supreme Court in Warrantless GPS Tracking Case Offers Little Guidance in Consumer Privacy Context*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Jan. 24, 2012), http://www.hldataprotection.com/2012/01/articles/consumer-privacy/supreme-court-decision-in-warrantless-gps-tracking-case-offers-little-guidance-in-consumer-privacy-context/; *see also* Dominic Rushe, *Google: Don't Expect Privacy When Sending to Gmail*, GUARDIAN (Aug. 14, 2013), http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit.

125. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE EXECUTIVE OFFICE OF THE PRESIDENT (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter Privacy Bill of Rights].

126. *Id.* (emphasis added).

127. Robert Gellman, *Fair Information Practices: A Basic History* (Aug. 3, 2012), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf; *see also* Memorandum, Hugo Teufel III, Chief Privacy Officer, Dep't of Homeland Security, Privacy Policy Guidance Memorandum (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

128. Katz v. United States, 389 U.S. 347 (1967).

129. Gellman, *supra* note 127.

130. *Id.*

1974,[131] which governs the collection and use of data by federal agencies, and over time, were further embraced as the basis of global privacy law.[132]

The FIPPS have a degree of flexibility built into their application, and at different times, different principles have been emphasized ranging from the rights of individuals to the obligations of data collectors. However, from their earliest formulation, the FIPPs stressed the ability for individuals (1) to find out what information exists about them in records and how that information is used, (2) to prevent information obtained for one purpose to be used or made available for other purposes without consent, and (3) to be allowed to correct or amend identifiable records.[133]

In the United States, the chief privacy regulator, the Federal Trade Commission (FTC) embraces notice as the must "fundamental" principle of privacy protection.[134] In the process, the FTC has either "watered down" or excluded many traditional FIPPs.[135] Instead, individual control is largely governed through a notice-and-choice regime. In an ideal world, notice-and-choice captures the "personal adjustment process" or the decision-making process that Westin's definition envisions. Notice informs the individuals of the consequences of sharing their information, while choice ostensibly implements the individual's ultimate decision.

There is wide acknowledgement that the notice-and-choice framework has significant limitations at best, and at worst, provides only the barest illusion of control. As the President's Council of Advisors on Science and Technology describes it, only "in some fantasy world" do individuals "actually read these notices, understand their legal implications (consulting their attorneys if necessary), negotiate with other providers of similar services to get better privacy treatment, and only then click to indicate their consent."[136] Vast majorities do not read privacy policies—nor would they have the time to,[137] and studies have shown that privacy choices can be easily manipulated.[138] Former FTC Chairman

---

131. Privacy Act of 1974, 5 U.S.C. § 552(a) (2009).

132. Gellman, *supra* note 127, at 5.

133. DEPT. OF HEALTH, EDUCATION, AND WELFARE, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973) [hereinafter HEW Report], *available at* http://epic.org/privacy/hew1973report/.

134. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (1998).

135. Gellman supra note 127, at 11; *see also* Fred H. Cate, *The Failure of Fair Information Practice Principles*, in CONSUMER PROTECTION IN THE AGE OF INFORMATION ECONOMY 343 (Jane K. Winn ed., 2006), *available at* http://ssrn.com/abstract=1156972.

136. EXECUTIVE OFFICE OF THE PRESIDENT, PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (2014) [hereinafter PCAST].

137. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR THE INFO. SOC'Y 543 (2008).

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

Jon Liebowitz even conceded that "notice and choice" has not "worked quite as well as we would like."[139]

Control can—and should—mean more than rote notice-and-choice. The Consumer Privacy Bill of Rights suggests that consumers be given usable and accessible mechanisms to implement their choices that are calibrated to the sensitivity of the data being collected and the sensitivity of the potential uses of that information[140]. However, calls for better "user empowerment" or "privacy management" tools are not new,[141] and as a practical matter, entities ranging from social networks like Facebook to data brokers like Acxiom offer users various dashboards to give users some ability to declare their own preferences and terms of engagement.

But meaningful choice faces numerous cognitive hurdles. An October 2012 piece in the Harvard Business Review posits that individuals should only part with 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."[142] However, requiring individuals to do homework just to browse the Internet is a large ask. As discussed above, individuals neither read nor understand the average privacy policy or terms of use. Even assuming they did, it would still be impossible to understand the motives of third-parties. Truly informed choices are hard to achieve, and the status quo is a world where individuals frequently consent to the collection, use, and disclosure of their personal information when it is not in their self-interest.[143]

III. BIG DATA'S RELATIONSHIP WITH PRIVACY

Conceptions of privacy as secrecy or control break down when intimate details of our lives can be revealed simply in the course of carrying out mundane tasks. Since the revelation several years ago that Target was able to predict a teenager's pregnancy before her family was even aware of it,[144] it has become

---

139. Fred Cate, *Looking Beyond Notice and Choice*, PRIVACY & SECURITY LAW REPORT (Mar. 29, 2010), *available at* http://www.hunton.com/files/Publication/f69663d7-4348-4dac-b448-3b6c4687345e/Presentation/PublicationAttachment/dfdad615-e631-49c6-9499-ead6c2ada0c5/Looking_Beyond_Notice_and_Choice_3.10.pdf.

140. Privacy Bill of Rights, *supra* note 125.

141. Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273 (2012) (discussing the rise and fall of the P3P tool); *see also* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 243-51 (2013) (advocating for the "featurization" of data).

142. 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.

143. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1895 (2013).

144. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012,

apparent that corporate America, as well as government authorities, know far more about individual citizens than they let on. Even where individuals take affirmative steps to keep information secret or to tightly control it, privacy has given way to transparency.

Recently, another woman went to great lengths to try and hide her pregnancy from data collectors.[145] As the Target example illustrates, identifying pregnant consumers is a particular high priority—not only are pregnant women valuable from a data perspective,[146] but the arrival of children can be a potent time to lock in customer loyalty.[147] In order to hide her pregnancy, Janet Vertesi had to not only avoid social networks, but ensure her friends and family *also* made no mention about her pregnancy online.[148] To look for baby-information online, she relied on Tor, the anonymous web browser.[149] She relied on cash for any baby-related purchases, avoiding credit cards and store-loyalty cards.[150] While this protected her privacy from a consumer-facing perspective, her activities also raised red flags that pointed to potential criminal activity.[151] For example, when her husband attempted to buy $500 in gift cards with cash, a notice from Rite Aid informed him the company had a legal obligation to report excessive transactions to law enforcement.[152]

Meaningful secrecy has become impossible, and controls are increasingly inadequate—or confusing and unused.[153] In 1996, science-fiction author David Brin posited the rise of the "Transparent Society," where the proliferation of smaller and smaller surveillance devices would give society the choice between either an illusion of privacy or a system of accountability enforced by everyone watching everyone.[154] While the transparent society has itself been criticized for not *recognizing* unequal allocation of power and authority (e.g., in the relationship between citizen and law enforcement or employee and employer),[155] Brin's point that we move beyond illusions of privacy is important. Evgeny Morozov castigates privacy advocates for focusing on rethinking privacy

---

http://www.nytimes.com/2012/02/19/magazine/shopping-habits.ht.

145. Matt Petronzio, *How One Woman Hid Her Pregnancy From Big Data*, MASHABLE (Apr. 26, 2014), http://mashable.com/2014/04/26/big-data-pregnancy/.

146. *Id.* (According to Vertesi, the average value of a person's marketing data is just ten cents, but a pregnant woman's is worth $1.50.).

147. *See generally id.*

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

153. *See generally* JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014).

154. David Brin, *The Transparent Society*, WIRED (Dec. 1996), *available at* http://archive.wired.com/wired/archive/4.12/fftransparent.html?topic=&topic_set=.

155. Bruce Schneier, *The Myth of the "Transparent Society,"* SCHNEIER ON SECURITY (Mar. 6, 2008), https://www.schneier.com/essay-208.html.

controls, when privacy debates instead need to be infused with larger ethical principles.[156]

Our current reality more closely captures Brin's notion of an illusion of privacy without accountability.[157] Our legal and policy frameworks have clung to antiquated conceptions of privacy even as activities within the public and private sectors have become increasingly opaque while individuals more transparent. The past year's revelations of NSA surveillance programs provide a stark illustration of how one-sided our transparent society has become.[158] Despite repeated assurances from government officials that the programs were "under very strict supervision by all three branches of government,"[159] at different times it has been demonstrated that Congress had been caught largely unaware.[160] This accountability breakdown also exists within the judiciary, as well as within the executive branch itself.[161]

A chain of misunderstandings within the Department of Justice ultimately misled the U.S. Supreme Court about a key fact in *Clapper v. Amnesty International*, which considered warrantless surveillance under Section 702 of the FISA Amendments Act of 2008.[162] In *Clapper*, a collection of U.S. lawyers and journalists had sued alleging that their electronic exchanges with overseas contacts were being monitored without a warrant.[163] Section 702 would eventually be revealed as the authority underlying NSA PRISM program, which facilitates extensive surveillance of foreigners and can also incidentally acquire information about U.S. citizens.[164] In February 2013, the U.S. Supreme Court avoided the underlying privacy questions and dismissed *Clapper* on standing grounds, asserting that it was "speculative whether the Government will imminently target communications to which respondents are parties."[165] Though

---

156. Evygeny Morozov, *The Real Privacy Problem*, MIT TECH. REV. (Oct 22, 2013), http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/ (viewing the ethical need for privacy to require "sabotag[ing] the system," and he would likely not view proposals to respect context or engage in data use-based considerations to adequately protect privacy).

157. *See* Brin, *supra* note 154.

158. Barack Obama, President, United States, Remarks on NSA (June 7, 2013), *available at* http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/ (describing the NSA surveillance program).

159. *Id.*

160. Darren Samuelsohn, *Hill Draws Criticism Over NSA Oversight*, POLITICO (Mar. 2, 2014, 10:14 PM), http://www.politico.com/story/2014/03/hill-draws-criticism-over-nsa-oversight-104151.html.

161. *See id.* (explaining that blame has been placed on a variety of entities and individuals).

162. Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013).

163. *Id.* at 1145.

164. Glenn Greenwald, *NSA Prism Program Taps Into User Data Of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

165. *Clapper*, 133 S. Ct. at 1148.

it would be subsequently revealed that the PRISM program likely did monitor the parties in *Clapper*, the U.S. Supreme Court had accepted assurances from the Solicitor General that another party could have standing because prosecutors would "provide advance notice" to anyone prosecuted with evidence derived from surveillance under the 2008 law.[166] However, this was not true at the time, and as was subsequently reported,[167] there appears to have been significant confusion within the Department of Justice as to what prosecutorial practice actually was.[168]

Lest anyone believe this sort of confusion—or semantic doublespeak—is only present in government surveillance debates, efforts by consumer groups and industry to establish a "Do Not Track" (DNT) standard reveal similar problems.[169] The basic idea behind DNT is that it would provide an easy-to-use browser setting to allow consumers to limit the tracking of their activities across websites.[170] In February 2012, the White House Consumer Privacy Bill of Rights lauded DNT as a "mechanism [that] allow[s] consumers to exercise *some* control over how third parties use personal data or whether they receive it at all."[171] But there remains no consensus over what DNT means and thus, little progress has been made in offering consumers *any* control. The advertising industry, for example, interprets DNT to refer only to prohibition on targeted advertising.[172] Their self-regulatory solution allows consumers to request not to be tracked, but this preference is reflected only by declining to show that consumer personalized advertising on-line. Advertisers and websites remain free to still collect data about users, i.e., "track" them, as well as sell this information.[173]

In January 2014, in the wake of one headline after another about NSA surveillance, data brokers, and big data, President Obama called for a

---

166. Brief for Petitioner at 8, Clapper v. Amnesty International, 133 S. Ct. 1138 (2013) (No. 11-1025), *available at* http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/briefs/11-1025_petitioner.authcheckdam.pdf.

167. Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=0; *see also* Dan Novack, *DOJ Still Ducking Scrutiny After Misleading Supreme Court on Surveillance* (Feb. 26, 2014, 8:12 PM), https://firstlook.org/theintercept/2014/02/26/doj-still-ducking-scrutiny/.

168. Savage, *supra* note 167.

169. *See generally* Omer Tene & J. Trevor Hughes, *The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study*, 66 MAINE L. REV. 438 (2014).

170. *See* All About Do Not Track (DNT), http://www.allaboutdnt.com (last visited October 13, 2014).

171. Privacy Bill of Rights, *supra* note 125, at 12 (emphasis added).

172. Alexis C. Madrigal, *The Advertising Industry's Definition of "Do Not Track" Doesn't Make Sense,* THE ATLANTIC (Mar. 30, 2012), http://www.theatlantic.com/technology/archive/2012/03/the-advertising-industrys-definition-of-do-not-track-doesnt-make-sense/255285/.

173. Sarah A. Downey, *Why Do Not Track Really Means Do Not Target (and Doesn't Protect Your Privacy on Facebook)*, THE ONLINE PRIVACY BLOG (Feb. 28, 2012), http://www.abine.com/blog/2012/do-not-track-means-do-not-target/.

comprehensive review of how big data impacts individual privacy.[174] The resulting White House Big Data Review can be expected to set the tone for tone for future conversations about how to weigh big data against privacy. The two reports that emerged, *Big Data: Seizing Opportunities, Preserving Values*, by John Podesta, and a second report, *Big Data and Privacy: A Technological Perspective*, by the President's Counsel of Advisors on Science and Technology (PCAST), point to a future where secrecy and control are replaced by concepts like respect for context and responsible use.[175]

IV. EVOLUTIONS IN PRIVACY THINKING

Much of prior privacy thinking was binary.[176] Individuals either had a reasonable expectation of privacy, or they did not.[177] Users either consented or not.[178] Yet binary conceptions of privacy not only have done a disservice to individual's subjective and objective privacy beliefs, but it oversimplifies that spectrum of meanings and values of privacy.[179] Increasingly, policy makers are considering new privacy formulations that offer a more holistic review of different privacy values.[180] As I will discuss, new conceptions of privacy revolving around respect for context and responsible use will require difficult decisions—and will ask individuals to put their privacy into other parties' hands.

A. Respect for Context

Helen Nissenbaum's theory of contextual integrity has become especially important in privacy thinking.[181] Context views privacy as neither a right to secrecy nor a right to control, but rather views privacy as a right to the appropriate flow of personal information.[182] According to Nissenbaum, privacy can still be posited as an important human right or legal value, but viewing

---

174. John Podesta, *Big Data and the Future of Privacy*, THE WHITE HOUSE BLOG (Jan. 23, 2014, 3:30 PM), http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy.

175. EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 55-57 (2014) [hereinafter BIG DATA REPORT], *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf; *see also* PCAST, *supra* note 136, at 41.

176. *See, e.g.*, Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 647-48 (2013) (discussing binary distinctions of privacy in various legal formulations).

177. *Id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. *See, e.g.*, Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy*, ATLANTIC (Mar. 29, 2012, 4:44 PM), http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/.

182. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 127 (2010).

privacy through the lens of contextual integrity admits that what exactly privacy amounts to varies from context to context.[183]

Respect for context takes into consideration the informational norms of society, and admits that how individuals act and share information varies depending upon different relationships and power structures, among other things.[184] Social contexts can include family and friend relationships or the workplace, and the different types of interactions individuals have with doctors, pastors, or professors.[185]

The context in which data is collected and used has become an important part of understanding individual's privacy expectations. Context has become a key principle in both the 2012 Consumer Privacy Bill of Rights and the FTC's recent Privacy Framework.[186] The Consumer Privacy Bill of Rights explicitly declares that "[c]onsumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[187] A theory of context helps to explain, for example, why parents are upset over suggestions that their school children's education data is being used for marketing or advertising purposes,[188] or why the public widely approves of Amazon using their data to power the site's purchase recommendation engine.[189] The philosophical challenge facing organizations and policy makers is that respect for context requires an appreciation for ever-shifting social and cultural norms.[190] Context rests on a number of subjective variables such as an individual's level of trust in an organization and his perception of the

---

183. *Id.*

184. *Id.* at 132.

185. *Id.*

186. Privacy Bill of Rights, *supra* note 125, at 15; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 38-39 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

187. Privacy Bill of Rights, *supra* note 125, at 15.

188. Crista Sumanik, *National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared: Americans Overwhelmingly Support Reforms to Protect Students, Including Increased Transparency, Tighter Security Standards, and More Restrictions on Companies and Cloud Services, Common Sense Media* (Jan. 22, 2014), https://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern.

189. Stephanie Miller, *Privacy and Trust: Is it Time to Do it Like Amazon?*, DMA (Jan. 27, 2014), http://thedma.org/advance/data-driven-marketing-ideas/privacy-amp-trust-is-it-time-to-quotdo-it-like-amazonquot/.

190. Carolyn Nguyen, Director, Microsoft Technology Policy Group, Contextual Privacy, Address at the FTC Internet of Things Workshop (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

value he receives from the use of his information.[191]

While context has been warmly embraced in principle, in practice, much more work by academics, industry, and policy makers is needed in order to properly frame and define this principle. Even as the White House Consumer Privacy Bill of Rights highlights the importance of context, Nissenbaum notes that both the accompanying White House report, *Consumer Privacy in a Networked World*, and later comment and reaction relied upon a variety of different interpretations of context.[192] She highlights five prominent interpretations of context: (1) context as determined by purpose specification; (2) context as determined by technology, or platform; (3) context as determined by business sector, or industry; (4) context as determined by business model; and, finally (5) context as determined by social sphere.[193] Context as defined by either industry efforts to specify how they intend to use data *or* by industry determinations in general do little to promote respect for individual privacy, while context as determined by business model or technology remain open-ended.[194] Nissenbaum reiterates that respect for context lacks analytical rigor if it does not take the social sphere into account—it also results in a much diminished notion of privacy, as well.[195]

These different interpretations are particularly significant because privacy advocates view the notion of context as being generally pro-privacy.[196] Because of this, context both complements and is in tension with emerging frameworks that protect privacy through responsible data use.[197]

B. Responsible Use-Based Approaches

The untapped value of big data has spurred a number of organizations to

---

191. *Id.*

192. Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't*, BERKLEY LAW (May 24, 2013, 9:31 PM), privacylaw.berkeleylawblogs.org/2013/05/24/helen-nissenbaum-respect-for-context-as-a-benchmark-for-privacy-online-what-it-is-and-isnt-2/ [hereinafter Nissenbaum, *Respect for Context*, BERKLEY LAW]. Nissenbaum's article on this subject remains a work-in-progress, though she has discussed formulations of these interpretations at a number of different venues. *E.g.*, Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't*, *in* THE FUTURES OF PRIVACY 19 (Carine Dartiguepeyrou ed., 2014), *available at* http://cvpip.wp.mines-telecom.fr/files/2014/02/14-02-The-futur-of-privacy-cahier-de-prospective.pdf [hereinafter Nissenbaum, *Respect for Context*, *in* THE FUTURES OF PRIVACY].

193. Nissenbaum, *Respect for Context*, BERKLEY LAW, *supra* note 192.

194. *See* Nissenbaum, *Respect for Context*, *in* THE FUTURES OF PRIVACY, *supra* note 192, at 27-28 .

195. *Id.* at 28.

196. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 89 (2013).

197. BIG DATA REPORT, *supra* note 175, at 56 (The White House Big Data Report recognizes this tension, *see infra* Part IV.B.).

move from privacy protections based on how information is *collected* toward how information is *used*.[198] Big data promises much value from innovative secondary uses of information—including breakthroughs in medicine, data security, or energy usage—that are impossible to account for under current notice-and-choice models.[199] Both reports that emerged out of the White House big data review support a focus on the merits of a use-based approach to privacy; the report by John Podesta specifically emphasizes the value of responsible data use:

> Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[200]

However, the White House-Podesta report also attempts to harmonize use-based approaches with a contextual approach to privacy, stating that a focus on use "does not mean ignoring the context of collection."[201] The report goes on to state that "[p]art of using data responsibly could mean respecting the circumstances of its original collection," and it continues, suggesting that a "no surprises" rule should govern how entities use data.[202]

However, context is largely missing from use-based path forward proposed by Scott Charney, who runs the influential Trustworthy Computing Group at Microsoft. Charney emphasizes the shift in privacy burden from individuals to

---

198. *See* Polonetsky et al., *supra* note 39, at 7; *see also* WORLD ECONOMIC FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE (2013), *available at* http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage; *see also* MICROSOFT, EVOLVING PRIVACY MODELS (2014), *available at* http://download.microsoft.com/download/1/5/4/154763A0-80F8-41C8-BE52-80E284A0FBA9/Evolving-Privacy-Models.pdf.

199. Fred H. Cate & Viktor Mayer-Schönberger, *Data Use and Impact Global Workshop*, CTR. FOR INFO. POLICY RESEARCH AND CTR. FOR APPLIED CYBERSECURITY RESEARCH INDIANA UNIVERSITY (Dec. 1, 2013), http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf; *see also* SCOTT CHARNEY, TRUSTWORTHY COMPUTING NEXT (2012); Scott Charney, *The Evolving Pursuit of Privacy*, HUFFINGTON POST (Apr. 10, 2014 3:04 PM), http://www.huffingtonpost.com/scott-charney/the-evolving-pursuit-of-p_b_5120518.html ("We can inform individuals what will happen to their data today, but what happens when organizations develop new services or data use models?").

200. BIG DATA REPORT, *supra* note 175.

201. *Id.*

202. *Id.*; *see also* Jedidiah Bracy, *Making the Case for Surprise Minimization*, IAPP PRIVACY PERSPECTIVES (Apr. 11, 2014), https://www.privacyassociation.org/privacy_perspectives/post/making_the_case_for_surprise_minimization (exploring how privacy best practices are increasingly about surprise minimization).

organizations through new accountability and enforcement mechanisms.[203] Ideally, a use-based approach aspires to consensus around broadly acceptable data uses, allowing "uses where reasonable minds can differ can stand out more prominently" and allowing stakeholders to focus on "managing the risks associated with these activities."[204] The larger goal in shifting responsibility in this fashion seeks to not only replace our current compliance-based privacy framework, but to actively promote better data stewardship, as well.[205]

Regulators and privacy advocates are skeptical. While not opposed to accountability and enforcement in principle, no one is quite sure what these new accountability mechanisms should look like in a world of big data. Ryan Calo has proposed formalized review mechanisms roughly analogous to the function institutional review boards play in human testing research,[206] while Mayer-Schönberger and Cukier have called for big data "algorithmists" that could evaluate the selection of data sources, analytical tools, and any resulting interpretations.[207]

Moreover, there are worries that this approach places too much power into the hands of companies.[208] Use-based approaches necessarily minimize the role and rights of the individual, and in effect, create a business-centric form of privacy paternalism.[209] The PCAST big data report is particularly supportive of

---

203. CHARNEY, *supra* note 199; *see also* Charney, *The Evolving Pursuit of Privacy*, *supra* note 199.

204. CHARNEY, *supra* note 199.

205. *See* Cate & Mayer-Schönberger, *supra* note 199.

206. Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 STAN. L. REV. 97 (2013).

207. Cate & Mayer-Schoenberger, *supra* note 199.

208. *See*, *e.g.*, Will Gore, *Google and Its Like Are Now Masters of Our Universe—By Order of the European Court*, INDEPENDENT (May 18, 2014), http://www.independent.co.uk/voices/google-and-its-like-are-now-masters-of-our-universe--by-order-of-the-european-court-9392372.html (The European Court of Justice's recent ruling that Google must implement procedures allowing users to request the deletion of certain information was hailed as a tremendous victory for privacy, but it may actually place tremendous authority to make decisions about what should and should not be "private" into the hands of a corporation.). Ann Cavoukian, *So Glad You Didn't Say That! A Response to Viktor Mayer-Schoenberger*, IAPP (Jan. 16, 2014), https://www.privacyassociation.org/privacy_perspectives/post/so_glad_you_didnt_say_that_a_response_to_viktor_mayer_schoenberger (According to Ann Cavoukian, Information and Privacy Commissioner of Ontario, regulator's resources "are already stretched to the limit, with no additional resources being allocated for such enforcement. And with the massive growth in online connectivity and ubiquitous computing, we would barely see the tip of the iceberg of the privacy infractions that would arise."); *see also* Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1205 (2003) (for criticism of the FTC's privacy enforcement actions generally); *see also EPIC v. FTC (Enforcement of the Google Consent Order)*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org/privacy/ftc/google/consent-order.html (last visited Sept. 10, 2014).

209. Justin Brookman*, Corporate Accountability Is Important, But Consumers Still Need*

a responsible use framework, and it largely assumes that privacy *should* be sacrificed in order to allow big data to pursue improvements in convenience and security in everyday life.[210] Evoking the transparent society, PCAST imagines a future where a young woman prepares for a business trip where her bags are tracked from bedroom to hotel with RFID tags, cameras on streetlights observe her home so she can leave her bags outside her front door, and amusingly, the Transportation Security Agency at the airport is hardly necessary because any signs the woman was "deranged and dangerous" would "already have been tracked, detected, and acted on."[211] This future, PCAST concedes, "seems creepy to us" today, but PCAST assumes individuals will accept a "different balance" in the future.[212]

V. TRUST BUT VERIFY

"Creepy" has been an oft-used (and oft-lamented) descriptor of technological changes.[213] Perhaps as a result, creepiness tends to go hand-in-hand with discussions about big data, as well as various implementations of the Internet of Things.[214] Target's predictive abilities were considered "creepy."[215] The past year has seen an endless parade of "scary" and "weird" things that the NSA can now do.[216] Connected "smart" cars may be the next "privacy nightmare,"[217] while

---

Meaningful Control, IAPP PRIVACY PERSPECTIVES (May 8, 2014), https://www.privacyassociation.org/privacy_perspectives/post/corporate_accountability_is_important_but_consumers_still_need_meaningful_c.

210. *The President's Big Data Report by PCAST-Examining Conflicts of Interest,* CTR. FOR DIGITAL DEMOCRACY (May 7, 2014), http://www.democraticmedia.org/presidents-big-data-report-pcast-examining-conflicts-interest (The Center for Digital Democracy notes that a number of the members of PCAST have direct connections to major technology companies and data collectors.).

211. PCAST, *supra* note 136, at 17-18.

212. *Id.*; *see also* G.S. Hans, *Big Data Report Shows Privacy Matters*, CTR. DEMOCRACY & TECH. (May 2, 2014), https://cdt.org/blog/big-data-report-shows-privacy-matters/ (providing additional criticism of PCAST's hypothetical).

213. Farhad Manjoo, *The End of the Echo Chamber*, SLATE (Jan. 17, 2012,11:00 AM), http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html; *see also* Adam Thierer, *On "Creepiness" as the Standard of Review in Privacy Debates*, The Tech. Liberation Front (Dec. 13, 2011), http://techliberation.com/2011/12/13/on-creepiness-as-the-standard-of-review-in-privacy-debates/ (Thierer laments that "creepiness" is a "crappy standard by which to judge privacy matters.").

214. Future of Privacy Forum, *Public Comments, Big Data RFI* (Mar. 31, 2014), http://www.futureofprivacy.org/wp-content/uploads/OSTP-Big-Data-Review-Comments.pdf.

215. *Id.*

216. Jody Avirgan, *Every Scary, Weird Thing We Know the NSA Can Do*, FUTURE TENSE (Jan. 17, 2014, 5:00 PM), http://www.slate.com/blogs/future_tense/2014/01/17/nsa_surveillance_reform_every_scary_weird_thing_we_know_the_agency_can_do.html.

217. Ronald D. White, *Car Black Boxes: Privacy Nightmare or a Safety Measure?*, LOS ANGELES TIMES (Feb. 15, 2013), http://articles.latimes.com/2013/feb/15/autos/la-fi-hy-advocates-

Google offers tips on how to avoid being "creepy" with Google Glass.[218] In fact, Google's own policy "is to get right up to the creepy line and not cross it."[219] What is creepiness? Jules Polonetsky and Omer Tene suggest that creepy behaviors are connected with activity that

> is *not exactly* harmful, does not circumvent privacy settings, and does not technically exceed the purposes for which data were collected. They usually involve either the deployment of a new technology, such as a feature that eliminates obscurity, or a new use of an existing technology, such as an unexpected data use or customization. In certain cases, creepy behavior pushes against traditional social norms; in others, it exposes a rift between the norms of engineers and marketing professionals and those of the public at large . . . .[220]

Creepiness directly limits the ability of an individual to feel comfortable or in control of his life.[221] According to Francis McAndrew and Sara Koehnke, feeling "creeped out" is "an evolved adaptive emotional response to ambiguity about the presence of threat that enables us to maintain vigilance during times of uncertainty."[222]

Creepiness is inherently subjective, and as a result, creepy behaviors are detrimental to the development of any trust-based relationship—whether between friends, consumer and company, or government and citizen.[223] Increasingly, trust is at a premium. Polls routinely show, for example, that even as Americans have not gone off the grid en masse, they do not trust either private companies[224] or the

---

say-car-black-boxes-could-become-a-privacy-nightmare-20130215; *see also* Kashmir Hill, *The Big Privacy Takeaway From Tesla vs. The New York Times*, FORBES (Feb. 19, 2013, 2:45 PM), http://www.forbes.com/sites/kashmirhill/2013/02/19/the-big-privacy-takeaway-from-tesla-vs-the-new-york-times/ ("[M]y biggest takeaway was 'the frickin' car company knows when I'm running the heater?'").

218. Nick Bilton, *Google Offers a Guide to Not Being a 'Creepy' Google Glass Owner*, BITS (Feb. 19, 2014, 2:02 PM), http://bits.blogs.nytimes.com/2014/02/19/googles-guide-to-not-being-a-creepy-google-glass-owner/.

219. Bianca Bosker, *Eric Schmidt: Google's Policy Is To 'Get Right Up To The Creepy Line'*, THE HUFFINGTON POST (Oct. 4, 2010, 10:01 AM), http://www.huffingtonpost.com/2010/10/04/eric-schmidt-google-creepy_n_748915.html.

220. Tene & Polonetsky, *supra* note 196, at 61 (emphasis added).

221. Future of Privacy Forum, *supra* note 214.

222. Francis T. McAndrew & Sara S. Koehnke, (On the Nature of) Creepiness Poster presented at the Annual Meeting of the Society for Personality and Social Psychology, (Jan 18, 2013), *available at* http://www.academia.edu/2465121/Creepiness.

223. *See generally id.*; *see also* Joseph Jerome & Joseph Newman, *Video Games and Privacy: It's All About Trust*, GAMASUTRA (May 20, 2014, 2:43 PM), http://www.gamasutra.com/blogs/JosephJerome/20140520/217964/Video_Games_and_Privacy_Its_All_About_Trust.php.

224. Charlie Warzel, *Americans Still Don't Trust Facebook with their Privacy*, BUZZFEED (Apr. 3, 2014, 2:58 PM), http://www.buzzfeed.com/charliewarzel/americans-still-dont-trust-facebook-with-their-privacy; *see also* Kayla Tausche, *As Investors Fawn Over Facebook, Poll*

government[225] with their privacy. Over time, a loss of trust can impact not just a company's bottom-line, but have serious corrosive effects on society, as well.

Trust is essential for society.[226] And thus far, big data has played a harmful role from the perspective of enhancing trust. However, if it can move the future of privacy away from arbitrary binaries toward a more holistic understanding of privacy as a value spectrum, big data may yet be a boon to privacy conversations. In this regard, contextual privacy or a shift to responsible uses of data may force businesses and government to more carefully consider their actions. Certainly these approaches do not by themselves answer many of the normative questions that result from the collection and use of data, but they may provide constraints and structure to decision-making processes.[227]

A better approach to privacy is a start—and in many ways, trust is the flip side of the privacy coin.[228] According to Ilana Westerman, organizations ought to focus less on privacy and more on trust.[229] "Privacy professionals should become trust professionals and become involved in overall product creation," she writes, arguing that this will help engender trust and create value.[230] But getting society—and perhaps Captain America—to trust big data is a multistep process.

CONCLUSION

The big data privacy bogeyman will only be excised through a combination of accountability, transparency, and ultimately, public debate. Yet this is bigger than a mere privacy conversation. The fundamental problem posed by big data may be less a question of how it impacts our privacy and more that it upsets our society's sense of fairness. The debate around big data is often couched as something that implicates traditional privacy principles and that the uses and

---

Finds User Distrust, Apathy, CNBC (May 12, 2012, 12:05 AM), http://www.cnbc.com/id/47413410; *see also* Mat Honan, *The Case Against Google*, GIZMODO (Mar. 22, 2012, 12:19 PM), http://gizmodo.com/5895010/the-case-against-google.

225. *Just 11% Think NSA Less Likely Now to Monitor Phone Calls of Innocent Americans*, RASMUSSEN REPORTS (Aug. 12, 2013), http://www.rasmussenreports.com/public_content/politics/general_politics/august_2013/just_11_think_nsa_less_likely_now_to_monitor_phone_calls_of_innocent_americans.

226. *See* Bruce Schneier, *NSA Secrets Kill our Trust*, SCHNEIER ON SECURITY (July 31, 2013), https://www.schneier.com/essay-435.html.

227. *See* Andrew Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 649 (2013).

228. Ilana Westerman, *From Privacy to Trust Professionals*, IAPP (Mar. 25, 2013), https://www.privacyassociation.org/privacy_perspectives/post/from_privacy_to_trust_professionals.

229. *Id.*

230. *Id.*

inferences drawn from our data invade our privacy, but this obscures the larger public policy challenge. We are increasingly threatened by abstract or inchoate risks to our autonomy and the state of our society, and no one has established the necessary trust to lead the way forward.