The Myth of the Privacy Paradox

*Daniel J. Solove**

Abstract

In this Article, Professor Daniel Solove deconstructs and critiques the privacy paradox and the arguments made about it. The "privacy paradox" is the phenomenon where people say that they value privacy highly, yet in their behavior relinquish their personal data for very little in exchange or fail to use measures to protect their privacy.

Commentators typically make one of two types of arguments about the privacy paradox. On one side, the "behavior valuation argument" contends behavior is the best metric to evaluate how people actually value privacy. Behavior reveals that people ascribe a low value to privacy or readily trade it away for goods or services. The argument often goes on to contend that privacy regulation should be reduced.

On the other side, the "behavior distortion argument" suggests that people's behavior is not an accurate metric of preferences because behavior is distorted by biases and heuristics, manipulation and skewing, and other factors.

Professor Solove argues instead that the privacy paradox is a myth created by faulty logic. The behavior involved in privacy paradox studies involves people making decisions about risk in very specific contexts. In contrast, people's attitudes about their privacy concerns or how much they value privacy are much more general in nature. It is a leap in logic to generalize from people's risk decisions involving specific personal data in specific contexts to reach broader conclusions about how people value privacy.

The behavior in the privacy paradox studies does not lead to a conclusion for less regulation. On the other hand, minimizing behavioral distortion will not cure people's failure to protect their own privacy. Managing one's privacy is a vast, complex, and never-ending project that does not scale. Privacy regulation often seeks to give people more privacy self-management, but doing so will not protect privacy effectively. Professor Solove argues instead that privacy law should focus on regulating the architecture that structures the way information is used, maintained, and transferred.

Table of Contents

---

* John Marshall Harlan Research Professor of Law, The George Washington University Law School. For very helpful comments on this Article, I would like to thank Alessandro Acquisti, Danielle Citron, Donald Dripps, Michael Froomkin, Woodrow Hartzog, Chris Hoofnagle, and Paul Schwartz. Thanks to Jasmine Arooni and Shannon Sylvester for research assistance.

January 2021 Vol. 89 No. 1

INTRODUCTION

Many studies have shown that people's attitudes about privacy differ a lot from their behavior. In surveys, people say that they value privacy highly, yet they readily give away sensitive personal information for small discounts or tiny benefits—or sometimes for nothing at all.[1] People express strong concern about privacy yet fail to take easy and inexpensive steps to protect their privacy.[2] This phenomenon is known as the "privacy paradox."[3]

---

1 *See, e.g.*, Sarah Spiekermann, Jens Grossklags & Bettina Berendt, *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior*, *in* EC '01: PROCEEDINGS OF THE 3RD ACM CONFERENCE ON ELECTRONIC COMMERCE 38, 38–39, 45 (2001) (indicating that, despite the results of numerous surveys showing that people place a high value on their privacy, in a controlled study, online shoppers were willing to give up vast amounts of personal info when asked by an anthropomorphic 3-D shopping bot).

2 *See infra* notes 23–26 and accompanying text.

3 *See infra* Part I.

Why is the privacy paradox occurring? What should be done about it? What direction should privacy regulation take in light of the privacy paradox? Countless attempts have been made to examine and understand the paradox as well as propose recommendations for law and policy. A search of "privacy paradox" in Google Scholar produces more than 8,000 results.[4] The privacy paradox plays a significant role in debates about privacy and how it should be regulated.

Responses to the privacy paradox typically take one of two opposing sides. One side advances what I call the "behavior valuation argument." Commentators in this camp embrace the privacy paradox and argue that behavior more reliably indicates how much people value their privacy than their stated attitudes.[5] Because people trade their privacy for small rewards, the argument goes, their behavior reveals that they ascribe a low value to their privacy.[6] Proponents of the behavior valuation argument often go a step further; they contend that the privacy paradox suggests that privacy regulation should be weakened, curtailed, or not enacted.[7] The argument notes that privacy regulation is often sparked by people's stated concerns about privacy, but people's behavior indicates that these concerns are inflated and that people are readily trading off their privacy for the benefits of new technologies or for free or discounted goods and services.[8] Regulators should therefore be reluctant to interfere.

On the opposite side, commentators respond to the privacy paradox by trying to explain away the variance between attitudes and behavior. In what I call the "behavior distortion argument," commentators argue that the people's behavior is irrational or inconsistent with their actual preferences.[9] Commentators point to influences which distort people's behavior, such as biases and heuristics or manipulation and skewing. Behavior is thus not a reliable metric for how much people value their privacy. The implication for policy is that privacy regulation should attempt to reduce the distorting influences

---

4 Googling "Privacy Paradox," GOOGLE SCHOLAR, https://scholar.google.com/ [https://perma.cc/TRU8-CSFY] (type "Privacy Paradox" into Google Scholar; then view the number of search results).

5 *See infra* Part II.

6 *See, e.g.*, L. Gordon Crovitz, Opinion, *Privacy? We Got Over It*, WALL ST. J. (Aug. 25, 2008), http://online.wsj.com/article/SB121962391804567765.html [https://perma.cc/6NMX-83JF] ("[W]hatever we say about how much we value privacy, a close look at our actual behavior suggests we have gotten over it.").

7 *See infra* notes 51–60 and accompanying text.

8 *See infra* notes 51–60 and accompanying text.

9 *See infra* Part III.

on behavior so that people make choices more in line with their actual preferences.

This Article takes a different path—it argues that the privacy paradox is not a paradox. The privacy paradox does not need to be explained because it does not exist. When properly understood, behavior and attitudes about privacy are not out of alignment. The privacy paradox is essentially an illusion created by faulty logic, unwarranted generalizations, and conflated issues.

The Article begins with background about the privacy paradox and the opposing arguments in response to it. Part I discusses the privacy paradox. Part II examines the behavior valuation argument, and Part III explores the behavior distortion argument.

Part IV advances this Article's primary contention—the privacy paradox is a myth. Attitudes and behavior only appear to be in conflict; they actually involve different things. The behavior in the privacy paradox involves people making decisions about risk in very specific contexts. In contrast, people's attitudes about their privacy concerns or how much they value privacy are much more general in nature. The behavior valuation argument generalizes from people's risk decisions involving specific personal data in specific contexts to reach broader conclusions about how people value privacy. This generalization is a leap in logic; it does not follow from the behavior in the studies. Moreover, the behavior valuation argument often views people's sharing data with organizations as conflicting with their concerns about privacy. But "privacy" involves a plurality of different things that extend far beyond just keeping data secret.[10] A person does not surrender all privacy when sharing data with others. Many privacy protections remain in place.

More broadly, because behavior and attitudes regarding privacy are about different things, the fact that they do not align is not a discrepancy. It is not even clear that they can be brought into alignment. Depending upon which side one takes, it can be tempting to view behavior or attitudes as a more fixed reflection of people's true preferences, with the other being false or skewed. But behavior and attitudes are highly malleable and are quite different. Behavior involves risk decisions within specific contexts; it is always context dependent. Attitudes are more general views about value and can exist beyond specific contexts. The fact that attitudes and behavior about privacy diverge is not a paradox or even an inconsistency.

---

10 *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101–70 (2008).

Part V examines the policy and regulatory implications of the behavior exhibited in the privacy paradox. There is definitely a difference between attitudes and behavior, with people's attitudes reflecting a strong value for privacy and with their behavior of often failing to protect their own privacy and readily sharing personal data. What is the import of this behavior on policy and regulation?

This Article contends that the conclusion of the behavior valuation argument—that privacy regulation overvalues privacy and ought to be curtailed—is based on a series of conflated issues and faulty logic. Individual risk decisions in particular contexts indicate little about how people value their own privacy, which is distinct from how people value privacy in general. Further, the value of privacy cannot be determined empirically by examining individual valuations of privacy and cannot be reduced to a monetary figure based on specific transactions. Privacy's value is as a constitutive element in society, not a bartered good in the marketplace.

Regarding the behavior distortion argument, although the effort to counter the distorting influences on behavior is a laudable one, it unfortunately will be quite limited in achieving effective privacy protection. Even a rational decisionmaker without any undue influences on behavior will fail to make good assessments of privacy risks and fail to manage her privacy effectively.

The reason for people's failure to manage privacy effectively is based on the futility of what is called "privacy self-management."[11] Privacy self-management involves the various decisions people must make about their privacy and the tasks people are given the choice to do regarding their privacy, such as reading privacy policies, opting out, changing privacy settings, and so on.[12] Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively. The best people can do is manage their privacy haphazardly. People cannot learn enough about privacy risks to make informed decisions about their privacy. People will never gain sufficient knowledge of the ways in which personal data will be combined, aggregated, and analyzed over the years by thousands of organizations. Resignation is a rational response to the impossibility of privacy self-management.

Unfortunately, existing privacy regulation relies too heavily on privacy self-management as a means of privacy protection. For exam-

---

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

12 *See id.*

ple, the recent California Consumer Privacy Act[13] provides individuals with a series of rights to manage their privacy such as a right to find out about data collected about them and a right to opt out of the sale of their data.[14] When privacy regulation gives people more control over their personal data, and people fail to complete the tasks to exercise greater control, the behavior valuation argument cites this behavior as evidence that people don't really care about their privacy. However, doing countless tasks to exercise more control is an endless and impractical task—and the control is often illusory.

Therefore, this Article recommends taking privacy regulation in a different direction. Privacy regulation can be best strengthened by regulating in ways that do not rely on individuals managing their own privacy. Instead, privacy regulation should focus on regulating the architecture that structures the way information is used, maintained, and transferred.

I. The Privacy Paradox and Its Impact

The privacy paradox has been documented by countless scholars and commentators.[15] The phenomenon is based on experiments, surveys, or general observations about behavior.

Before the privacy paradox received its moniker, early studies revealed an inconsistency between stated privacy attitudes and people's behavior. A study conducted in 2000 by Sarah Spiekermann, Jens Grossklags, and Bettina Berendt compared participants' privacy preferences to the personal data they disclosed to an anthropomorphic chat bot while shopping online.[16] The researchers originally hypothesized that people who are more concerned about their privacy would be less detailed, forthcoming, and truthful when answering questions.[17] Instead, to the surprise of the researchers, "participants displayed a surprising readiness to reveal private and even highly personal information and to let themselves be 'drawn into' communication with the anthropomorphic 3-D bot."[18] The findings were particularly eye-opening because the "bot questions were designed to include many non-legitimate and unimportant personal questions."[19]

13 Cal. Civ. Code §§ 1798.100–.199 (West 2020).

14 *See id.*

15 *See supra* note 4 and accompanying text.

16 Spiekermann et al., *supra* note 1, at 38–39.

17 *See id.* at 42.

18 *Id.* at 45.

19 *Id.*

Furthermore, participants "had to sign that they agreed to the selling of their data to an anonymous entity."[20] The researchers noted:

> A majority of persons who participated in the shopping experiment disclosed so much information about themselves that a relatively revealing profile could be constructed on the basis of only one shopping session. This result is not only alarming in itself, but even more so given that for many participants this behavior stands in sharp contrast to their self-reported privacy attitude . . . .[21]

Subsequent studies reveal a similar inconsistency between people's privacy attitudes and behavior. A 2005 study by Bettina Berendt, Oliver Günther, and Sarah Spiekermann found that people "do not always act in line with their stated privacy preferences, giving away information about themselves without any compelling reason to do so."[22] A study by Alessandro Acquisti and Jens Grossklags revealed that nearly 90% of participants said they were "moderately or very concerned about privacy."[23] When examining behavior, many people admitted to not engaging in certain privacy-protective measures: "87.5 percent of individuals with high concerns toward the collection of offline identifying information (such as name and address) signed up for a loyalty card using their real identifying information."[24] Of people "who were particularly concerned about credit-card fraud and identity theft, only 25.9 percent used credit alert features."[25] Of the people who agreed that "privacy should be protected by each individual with the help of technology," a large number did not take certain privacy-protective technological measures: "62.5 percent never used encryption, 43.7 percent do not use email-filtering technologies, and 50.0 percent do not use shredders for documents to avoid leaking sensitive information."[26] A 2006 study by Alessandro Acquisti and Ralph Gross found a dichotomy between people's privacy concerns and Facebook use practices: "We detected little or no relation between participants' reported privacy attitudes and their likelihood of providing certain in-

---

20 *Id.*

21 *Id.*

22 Bettina Berendt, Oliver Günther & Sarah Spiekermann, *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, COMMC'NS ACM, Apr. 2005, at 101, 104.

23 Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SEC. & PRIV., Jan.–Feb. 2005, at 26, 28.

24 *Id.* at 29.

25 *Id.*

26 *Id.*

formation, even when controlling, separately, for male and female members."[27]

In 2007, the disconnect between attitudes and behavior was given a name—the "privacy paradox"—in an article called *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*.[28] The name stuck and became the common way of referring to the phenomenon.

Privacy paradox studies are now legion. For example, in a study conducted in Germany by Alastair Beresford, Dorothea Kübler, and Sören Preibusch, subjects were asked to purchase a DVD from one of two identical stores.[29] One store sold the DVDs for one Euro fewer than the other, but the cheaper store requested more sensitive data.[30] Both stores requested the subject's name, postal address, and email address.[31] The cheaper store, however, required date of birth and monthly income whereas the more expensive store required that users provide their year of birth and favorite color.[32] Despite 95% of subjects saying that they were "interested in the protection of their personal information" and 75% saying "that they have a very strong interest in data protection," nearly all subjects chose the store that offered the cheaper price but required more personal data.[33]

A study by several researchers at the University of Madeira compared people's stated privacy attitudes to their social media activity on Facebook and found "little correlation between participants' broader concern about privacy on Facebook and their actual posting practices: both the number of postings and the portion of those posts visible to a large audience appear to be independent of general privacy attitudes."[34]

---

27 ALESSANDRO ACQUISTI & RALPH GROSS, IMAGINED COMMUNITIES: AWARENESS, INFORMATION SHARING, AND PRIVACY ON THE FACEBOOK 15 (2006), https://dataprivacylab.org/dataprivacy/projects/facebook/facebook2.pdf [https://perma.cc/4V6A-5KCQ].

28 Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFFS. 100, 100–01 (2007).

29 Alastair R. Beresford, Dorothea Kübler & Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment*, 117 ECON. LETTERS 25, 25 (2012).

30 *Id.* at 26.

31 *Id.*

32 *Id.*

33 *Id.*

34 Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves & Vassilis Kostakos, *Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours*, *in* 13TH INTERNATIONAL CONFERENCE ON HUMAN-COMPUTER INTERACTION (INTERACT) 204, 211 (2011), https://www.researchgate.net/publication/221054832 [https://perma.cc/DC5U-ECRW].

A 2019 study involving smartphones and the downloading of mobile apps concluded that "despite the fact users still claim to be concerned about the potential misuse of their personal data, they remain unwilling to invest either the time and effort or the money necessary to protect their privacy."[35] The researchers examined participants' knowledge about privacy risks and found that increased knowledge did not correlate to increased privacy-protective behavior: "Despite their technical backgrounds and a higher than average understanding of privacy intrusion possibilities, participants were not willing to pay for their privacy."[36]

In their study of people's use of Gmail, Lior Strahilevitz and Matthew Kugler found results "consistent with the privacy paradox."[37] With the use of Gmail, a free email service which scans and analyzes the content of people's email, "the mean respondent rated automated content analysis of e-mails as 7.63 out of 10 on an intrusiveness scale."[38] However, only about thirty-five percent of respondents were willing to pay money for an email service that didn't scan and analyze content. Of those willing to pay, the median amount was just fifteen dollars per year. Only 3% of respondents would pay more than $120 per year.[39] Strahilevitz and Kugler concluded:

> Although consumers dislike automated content analysis, their willingness to pay for a version of Gmail that does not perform content analysis is quite limited, and there is no evidence to indicate that concerns about e-mail content analysis are presently driving consumers to choose substitute e-mail services that eschew e-mail content analysis.[40]

A number of studies demonstrate that people share personal data for low amounts of money. One study found that people provided

---

35 Susanne Barth, Menno D.T. de Jong, Marianne Junger, Pieter H. Hartel & Janina C. Roppelt, *Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors Among Users with Technical Knowledge, Privacy Awareness, and Financial Resources*, 41 TELEMATICS & INFORMATICS 55, 65 (2019).

36 *Id.* at 65.

37 Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S78 (2016).

> [C]onsumers seem to regard themselves as having authorized several controversial privacy-related practices by Google, Yahoo, and Facebook regardless of whether they were randomly assigned to read vague language that does not seem to explain the corporate practices in any meaningful detail or precise language that describes the corporate practices at issue with admirable clarity and specificity.

Id. at S92.

38 *Id.*

39 *Id.*

40 *Id.* at S93.

their online browsing history for seven Euros—or $8.25.[41] Another study found that people downloading smartphone apps were willing to pay only in the range of about one dollar to four dollars to avoid revealing to the app developer various types of personal data such as browsing histories, text messages, locations, and contact lists.[42] Grossklags and Acqusiti in another study found that "individuals almost always chose to sell their information and only rarely elect[ed] to protect their information even for values as little as $0.25."[43]

Some studies have produced findings that cut against the privacy paradox to at least some degree.[44] For example, a study by Eszter Hargittai and Eden Litt demonstrated that people with "higher Internet privacy skills are more likely to manage self-presentation online actively."[45] A study by danah boyd and Eszter Hargittai revealed that contrary to the privacy paradox, the teenagers they studied behaved in ways that indicated that they were not cavalier about their privacy: "Overall, our data show that far from being nonchalant and unconcerned about privacy matters, the majority of young adult users of Facebook are engaged with managing their privacy settings on the site at least to some extent."[46] In a study by Kirsten Martin, a "trust game experiment shows respondents are less willing to engage with a partner who violated privacy by utilizing an ad network as compared to one who used privacy preserving advertising, even when engagement is financially advantageous to the individual."[47] These studies, how-

41 Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini & Rodrigo de Oliveira, *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online*, *in* WWW '13: PROCEEDINGS OF THE 22ND INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 189 (2013).

42 Scott J. Savage & Donald M. Waldman, The Value of Online Privacy 6 (Oct. 16, 2013) (unpublished manuscript), https://ssrn.com/abstract=2341311 [https://perma.cc/QS72-P48D].

43 Jens Grossklags & Alessandro Acquisti, When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information 3 (June 7, 2007) (unpublished manuscript), http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEIS07.pdf [https://perma.cc/4QU6-MCA5].

44 Spyros Kokolakis cites to more than ten studies between 2008 and 2014 that "provide evidence that challenge the privacy paradox hypothesis." Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 COMPUTS. & SEC. 122, 126 (2017).

45 Eszter Hargittai & Eden Litt, *New Strategies For Employment? Internet Skills and Online Privacy Practices During People's Job Search*, IEEE SEC. & PRIV., May–June 2013, at 38, 43.

46 danah boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, 15 FIRST MONDAY (Aug. 2010), https://journals.uic.edu/ojs/index.php/fm/article/view/3086/2589 [https://perma.cc/98TT-LUDS].

47 Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms*, 30 BUS. ETHICS Q. 65, 87 (2020).

ever, have not done much to change the prevailing view about the existence of the privacy paradox.

II. Paradox Embraced: The Behavior Valuation Argument

Many commentators embrace the privacy paradox, drawing policy conclusions that privacy regulation should be lessened because people's behavior indicates that they do not value privacy very highly.[48]

The behavior valuation argument begins by contending that behavior is a more accurate measure of how people value privacy than their expressed attitudes. In economic literature, attitudes are referred to as "stated preferences" and behavior is referred to as "revealed preferences."[49] The behavior valuation argument posits that people's revealed preferences are a better indication of their actual preferences than their stated preferences.[50] The argument then contends that the privacy paradox demonstrates that people ascribe a fairly low value to their privacy or that they readily trade away their privacy for goods and services. Often, the argument advances a policy conclusion—privacy regulation is too often influenced by what people say about how much they value privacy or how concerned they are about privacy. Instead, they say, regulation should focus on behavior. People's revealed preferences indicate that they do not value their privacy very much, that they are not as concerned about privacy as they say they

48 *See, e.g.*, Crovitz, *supra* note 6 ("[W]hatever we say about how much we value privacy, a close look at our actual behavior suggests we have gotten over it."); L. Gordon Crovitz, *The 0.00002% Privacy Solution*, Wall St. J. (Mar. 28, 2011), https://www.wsj.com/articles/SB10001424052748704474804576222732361366712 [https://perma.cc/NAN9-4MZ5] ("If most Americans are happy to have Facebook accounts, knowingly trading personal information for other benefits, why is Washington so focused on new privacy laws? There is little evidence that people want new rules.").

49 *See* Wolfram Elsner, Torsten Heinrich & Henning Schwardt, The Microeconomics of Complex Economies: Evolutionary, Institutional, Neoclassical, and Complexity Perspectives § 6.4.1, at 139–40 (2015) ("The objective of the 'revealed preferences' approach was to remove all traces of utility and subjective (unobservable) states, or, unobservable preferences from explanations of consumer behavior . . . ."); Sabah Abdullah, Anil Markandya, & Paulo A.L.D. Nunes, *Introduction To Economic Valuation Methods*, *in* Research Tools in Natural Resource and Environmental Economics 143, 146 (Amitrajeet A. Batabyal & Peter Nijkamp eds., 2011).

50 The notion that revealed preferences are a better reflection of people's stated preferences originates in "revealed preference theory," which was developed by economist Paul Samuelson. *See* P.A. Samuelson, *A Note on the Pure Theory of Consumer's Behaviour*, 5 Economica 61, 62, 71 (1938); Paul A. Samuelson, *Consumption Theory in Terms of Revealed Preference*, 15 Economica 243, 243–44 (1948) (terming the foundation of his theory on consumer behavior as "revealed preference").

are, and that they are fine with trading their personal data for the rewards that companies are offering, such as free or discounted goods or services.

For example, law professor James Cooper argues: "[S]urveys, or what economists call 'stated preference,' tell us only that privacy, like most other things, has value. It cannot answer the real question for policymakers: How willing are consumers to swap personal data for other things they value? These tradeoffs are what matter."[51] Cooper then contends:

> Once the focus shifts to what economists call "revealed preference," or how consumers actually make tradeoffs, the story becomes quite different. Far from suggesting that consumers are reticent to engage the online ecosystem, the real world behavior illustrates consumers who are largely comfortable with the tradeoffs they make in their digital lives.[52]

Cooper also notes:

> Economic studies that have attempted to measure the value of personal data nearly universally find that even when consumers are fully aware of the trades they are making, they are willing to provide personal information for small amounts of compensation, or alternatively are only willing to pay very little to avoid personal data collection.[53]

Cooper concludes that "most consumers are comfortable with the typical bargain of sharing information with faceless servers in return for free content and services, such as email and social networking platforms."[54] Cooper urges the Federal Trade Commission ("FTC") to curtail its enforcement actions against companies for privacy violations:

> Until it confronts the empirical evidence, the FTC has not made the case that it, rather than the market, is better at mediating how consumers trade among competing values. Indeed, the FTC's posture appears to be based on the preferred mix of privacy and functionality for the most privacy sensitive consumers.[55]

---

51 JAMES C. COOPER, U.S. CHAMBER OF COM. FOUND., LESSONS FROM ANTITRUST: THE PATH TO A MORE COHERENT PRIVACY POLICY 2 (2017), https://www.uschamberfoundation.org/reports/lessons-antitrust-path-more-coherent-privacy-policy [https://perma.cc/MZ4T-2LRH].

52 *Id.* at 3.

53 *Id.*

54 *Id.*

55 *Id.* at 4.

In another article, Cooper, writing alongside former FTC Commissioner Joshua Wright, argues that "research finds that consumers are willing to accept small discounts and purchase recommendations in exchange for personal data."[56] The authors note that the results of the studies "are consistent with real world behavior in which consumers increasingly participate in online activities that reveal personal data to both known and unknown parties."[57] Based on the privacy paradox, Cooper and Wright conclude that "most consumers are comfortable with the typical bargain of sharing information with faceless servers in return for free content and services, such as e-mail and social networking platforms."[58] As a consequence, "the FTC's enforcement posture is likely to be too aggressive by failing to consider this empirical evidence and by placing too much weight on opinions from the most privacy-sensitive constituents."[59] They argue that the "FTC is using its bully pulpit to cajole companies into supplying too much privacy."[60]

Professor Omri Ben-Shahar writes that "people seem indifferent to Big Data collection. They share personal information on web platforms, knowing full well that it is collected by websites."[61] He goes on to note: "Even more striking is how little people value potential protections. Economists have found that people are willing to pay at most a few dollars to prevent their apps from harvesting data, such as the content of their text messages, stored on their smartphones."[62] Ben-Shahar reaches the conclusion that "Americans are nonchalant with respect to aggressive collection of their personal information."[63] In what he calls "the Grand Bargain in digital marketplace," free services are offered in exchange for personal data, and this bargain is "largely good news for consumers" because most people "don't mind paying with their data."[64] Only the "ticklish few—those who are more fussy about their privacy or have things to hide—can change the settings to

56 James C. Cooper & Joshua D. Wright, *The Missing Role of Economics in FTC Privacy Policy*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 465, 480 (Jules Polonetsky et al. eds., 2018).

57 *Id.* at 481.

58 *Id.* at 482.

59 *Id.*

60 *Id.*

61 Omri Ben-Shahar, *Privacy Is the New Money, Thanks To Big Data*, FORBES (Apr. 1, 2016, 3:48 PM), https://www.forbes.com/sites/omribenshahar/2016/04/01/privacy-is-the-new-money-thanks-to-big-data/#780f105f3fa2 [https://perma.cc/4UZT-KMM5].

62 *Id.*

63 *Id.*

64 *Id.*

turn off 'dataveillance' or buy anonymizing services for less than $100 per year."[65] Thus, Ben-Shahar concludes, "[t]here is no market failure in the Big Data sector and no proven need for protective regulation."[66]

Professor Eric Goldman points out that "consumers' stated privacy concerns diverge from what consumers do."[67] What matters more than what consumers say is "how much consumers will pay—in time or money—for the corresponding benefits. For now the cost-benefit ratio is tilted too high for consumers to spend much time or money on privacy."[68] He concludes: "Consumer behavior will tell companies what level of privacy to provide. Let the market continue unimpeded rather than chase phantom consumer fears through unnecessary regulation."[69]

Economics professor Caleb Fuller contends that the privacy paradox is because "individuals express greater demands for digital privacy when they are not forced to consider the opportunity cost of that choice."[70] Based on his study, Fuller argues that "[a]t least in the context of interacting with Google, the findings suggest that most individuals place relatively low values on privacy. A small expressed willingness to pay for privacy is consistent with behavior that seemingly disregards privacy threats."[71] He notes that the reason "why so many digital firms engage in information collection rather than adopting alternative methods of earning revenue" is because "consumers prefer exchanging information to exchanging money."[72] Fuller concludes that his study's "results should add a dose of humility to the impulse to regulate digital privacy."[73]

III. Paradox Explained: The Behavior Distortion Argument

There is another set of responses to the privacy paradox argument that takes an opposing path to the behavior valuation argument.

---

65 *Id.*

66 *Id.*

67 Eric Goldman, *The Privacy Hoax*, Forbes, Oct. 14, 2002, at 42, https://www.forbes.com/forbes/2002/1014/042.html#1991f49f2717 [https://perma.cc/SFN9-9VDA].

68 *Id.*

69 *Id.*

70 Caleb S. Fuller, *Is the Market for Digital Privacy a Failure?*, 180 Pub. Choice 353, 371 (2019).

71 *Id.*

72 *Id.*

73 *Id.*

In what I call the "behavior distortion argument," a group of commentators contend that behavior does not reliably reflect people's actual privacy preferences. These commentators seek to explain why people's behavior is not a reliable reflection of their true preferences. The behavior distortion argument points to a number of distorting influences on people's behavior, such as biases and heuristics, framing effects, and behavioral manipulation and skewing.

Interestingly, many of the commentators advancing the behavior distortion argument are the researchers whose studies are revealing the privacy paradox.[74] Some study authors appear rather alarmed and troubled by their findings, and they proffer explanations that try to make sense of the problematic behavior. For example, the Spiekermann, Grossklags, and Berendt study referenced earlier involving the anthropomorphic chat bot described its results as "problematic" and "alarming."[75] The authors concluded: "This result suggests that the development of privacy technologies needs to take a twist into a new direction: they need to be designed in such a way that they allow even moderately computer-literate online users to protect themselves from the degree of self-disclosure they are afraid of."[76]

This Part explores various explanations for the privacy paradox based on distorting influences on behavior.

A. Biases and Heuristics

Many scholars have attempted to explain the privacy paradox by pointing to a number of cognitive problems that provide an alternative rationale for people's cavalier behavior toward privacy. These cognitive problems were originally explored by pioneering scholars Amos Tversky and Daniel Kahneman, who termed them "heuristics and biases."[77] Tversky and Kahneman began their careers at Hebrew University of Jerusalem in the psychology department.[78] Starting in

---

74 *See, e.g.*, *supra* notes 23–26 and accompanying text (discussing work of Alessandro Acquisti and Jens Grossklags in advancing the privacy paradox theory); *infra* notes 85–87 and accompanying text (discussing work of Alessandro Acquisti and Jens Grossklags in advancing the behavior distortion argument).

75 Spiekermann et al., *supra* note 1, at 45.

76 *Id.* at 46.

77 Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCI. 1124, 1124 (1974); DANIEL KAHNEMAN, THINKING, FAST AND SLOW 8–9 (2011).

78 Cass R. Sunstein & Richard Thaler, *The Two Friends Who Changed How We Think About How We Think*, NEW YORKER (Dec. 7, 2016), https://www.newyorker.com/books/page-turner/the-two-friends-who-changed-how-we-think-about-how-we-think [https://perma.cc/XB47-22G8]. For more information about the friendship and work of Tversky and Kahneman see MICHAEL LEWIS, THE UNDOING PROJECT: A FRIENDSHIP THAT CHANGED OUR MINDS (2017).

the 1970s, their studies demonstrated that people make decisions in irrational, but consistent ways.[79] These decision-making problems were due to certain heuristics and biases that distorted people's ability to assess their options in a rational manner.[80] Their work debunked the concept of the rational person in economics; they showed that people made decisions in irrational ways that did not maximize their self-interest.[81] Economics has since embraced Tversky and Kahneman's work, which forms the bedrock of behavioral economics.[82] Kahneman went on to win the Nobel Prize in Economics.[83]

Drawing from the work of Tversky and Kahneman, various scholars focusing on the privacy paradox have pointed to a number of biases and heuristics to explain people's behavior.[84] For example, Alessandro Acquisti and Jens Grossklags contend that people are limited by "bounded rationality," which involves the difficulty of figuring out what to do in complex situations involving costs, benefits, and risks.[85] They also note that people tend to favor immediate gratification; people give up their data without considering the long term costs and consequences.[86] This cognitive tendency is often referred to as "hyperbolic discounting."[87]

Another cognitive explanation for why people readily share personal data is that they have an illusory feeling of control. An article by Laura Brandimarte, Alessandro Acquisti, and George Loewenstein argues that "people who feel in control of their disclosures may underestimate the level of risk that arises from other people's access and uncontrollable usage of their disclosed information, and respond by

---

79 Sunstein & Thaler, *supra* note 78.

80 Tversky & Kahneman, *supra* note 77, at 1124.

81 *See id.* at 1130; Sunstein & Thaler, *supra* note 78; Elizabeth Kolbert, *What Was I Thinking?*, NEW YORKER (Feb. 18, 2008), https://www.newyorker.com/magazine/2008/02/25/what-was-i-thinking [https://perma.cc/FC6X-EQ2T].

82 Sunstein & Thaler, *supra* note 78.

83 *Id.* Tversky did not win because he had died, and the prize is not awarded posthumously. *Id.*

84 In a survey of the privacy paradox literature, Susanne Barth and Menno de Jong list dozens of theories of cognitive phenomena that scholars have used to explain the privacy paradox. *See* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1040–43 (2017).

85 *See* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, *in* ECONOMICS OF INFORMATION SECURITY 165, 172–73 (L. Jean Camp & Stephen Lewis eds., 2004).

86 *See id.* at 174.

87 *Id.* at 173.

disclosing more."[88] In other words, people are more comfortable supplying personal data when they feel in control—even if that control is illusory.[89]

B. Framing Effects

People's decisions about privacy are quite malleable and often turn upon how choices are framed. For example, the timing of when privacy notices are presented significantly affects people's decisions to share personal data.[90] As Will Oremus notes, "[s]tudy after study has found that people's valuations of data privacy are driven less by rational assessments of the risks they face than by factors like the wording of the questions they're asked, the information they're given beforehand, and the range of choices they're presented."[91]

The "endowment effect" has a major impact on how people value privacy. The endowment effect involves people's tendency to ascribe more value to something when they risk losing it and less value to the same thing when they do not possess it but have the opportunity to obtain it.[92] A study by Angela Winegar and Cass Sunstein found that people are "willing to pay relatively little ($5 per month) for privacy, but demand[ ] much more ($80 per month) to give up privacy."[93] Winegar and Sunstein note that this is an "unusually large disparity" and a "kind of superendowment effect."[94]

A study by Alessandro Acquisti, Leslie K. John, and George Loewenstein found that "endowment effects powerfully influence individual privacy valuations."[95] The researchers noted: "The answers to

---

88 Laura Brandimarte, Alessandro Acquisti, & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, 4 Soc. Psychol. & Personality Sci. 340, 341 (2013).

89 Woodrow Hartzog contends that much of the controls provided on sites are "illusory." Woodrow Hartzog, *The Case Against Idealising Control*, 4 Eur. Data Prot. L. Rev. 423, 426 (2018).

90 Serge Egelman, Janice Tsai, Lorrie Faith Cranor, & Alessandro Acquisti, *Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators, in* CHI '09: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 319, 324 (Saul Greenberg et al. eds., 2009).

91 Will Oremus, *How Much Is Your Privacy Really Worth?*, OneZero (Sept. 17, 2019), https://onezero.medium.com/how-much-is-your-privacy-really-worth-421796dd9220 [https://perma.cc/MQY6-SVAQ].

92 *See* Daniel Kahneman, Jack L. Knetsch & Richard H. Thaler, *Experimental Tests of the Endowment Effect and the Coase Theorem*, 98 J. Pol. Econ. 1325 (1990).

93 A.G. Winegar & C.R. Sunstein, *How Much Is Data Privacy Worth? A Preliminary Investigation*, 42 J. Consumer Pol'y 425, 426 (2019).

94 *Id.*

95 Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. Legal Stud. 249, 269 (2013).

questions such as What is privacy worth? and Do people really care for privacy? depend not just on whom, but *how*, you ask."[96] The study also revealed significant effects based on the ordering of choices.[97]

C. Behavioral Manipulation and Skewing

Another explanation for the privacy paradox is that people's behavior is being manipulated by companies and skewed by technological design. Professor Siva Vaidhyanathan contends that people's privacy choices online "mean very little" because "the design of the system rigs it in favor of the interests of the company and against the interests of users."[98]

In his illuminating book, *Privacy's Blueprint*, Professor Woodrow Hartzog argues that "there are overwhelming incentives to design technologies in a way that maximizes the collection, use, and disclosure of personal information."[99] Hartzog notes that design "affects how something is perceived, functions, and is used."[100] He further points out: "Because people react to signals and constraints in predictable ways, the design of consumer technologies can manipulate its users into making certain decisions. Design affects our perceptions of relationships and risk. It also affects our behavior . . . ."[101]

As Professor Ari Waldman notes, the privacy paradox "reflects users responding in predictable ways to the ways in which platforms leverage design to take advantage of our cognitive limitations."[102] A team of researchers from Princeton University and the University of Chicago uses the term "dark patterns" to describe "interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make."[103]

---

96 *Id.* at 268 (emphasis added).

97 *Id.* at 267.

98 SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 84 (2011).

99 WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018).

100 *Id.* at 21.

101 *Id.* at 23.

102 Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105 (2020).

103 Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, *in* 3 PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION 81:1, 81:2 (Airi Lampien et al. eds., 2019).

Not all behavioral skewing occurs because of deliberate design choices. Skewing sometimes occurs just because technology changes the circumstances in which people live and act. For example, people today widely expose their personal data on social media sites and elsewhere. Although developers of social media platforms design them in ways that encourage more data sharing, another factor that leads to more data sharing involves the nature of technology. The internet makes it easier for people to share information without the normal elements that can make them fully comprehend the consequences. If people were put in a packed auditorium, would they say the same things they say online? Most likely not. When people post online, they do not see the hundreds of faces staring at them. Seeing all those people makes the consequences of speaking in the immediate moment more visceral—much more than just seeing a computer screen. People also say things online that they would never say to another person face to face.[104]

Ultimately, whether design is created deliberately to manipulate us or unwittingly skews our behavior, the end result is the same—people share data in ways that they might not otherwise have shared.

D. Misunderstandings and Lack of Knowledge

Many surveys ask people about their general preferences about privacy. But when people are asked questions to find out how much they understand the choices they are making with their personal data, their level of knowledge is often quite limited or they have significant misunderstandings.[105]

Professor Joseph Turow has performed numerous studies showing a knowledge gap where consumers falsely believe that rules ban uses and selling for information. In a typical finding by Turow, 75% of people incorrectly believed that "[w]hen a website has a privacy policy, it means the site will not share [their] information with other websites

104 *See* Jane Wakefield, *Why Are People So Mean to Each Other Online?*, BBC NEWS (Mar. 26, 2015), https://www.bbc.com/news/technology-31749753 [https://perma.cc/RUS4-PJCW].

105 *See* Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 342–44 (2016).

and companies."[106] In another of Turow's studies, people correctly answered only 30% of questions regarding their privacy online.[107]

Ignorance of privacy rules can even explain popular conceptions of consumer privacy behavior. For instance, in their article discussing Alan Westin's theory of privacy, Chris Hoofnagle and Jennifer Urban show that people who Westin categorized as privacy "unconcerned" or privacy "pragmatist" tended to falsely believe that protections were in place and were more ignorant of actual privacy rules and regulations than people Westin categorized as privacy "fundamentalists."[108] When informed of the gap between what consumers thought were the rules and the reality that legal protections did not exist, privacy pragmatists made decisions more consonant with privacy fundamentalists.[109]

A study by Professor Kirsten Marin demonstrated that people wrongly interpreted a privacy notice to be "more protective of consumer data than the actual notice included in the survey."[110] Martin found that "respondents projected the important factors to their privacy expectations onto the privacy notice. Privacy notices became a tabula rasa for users' privacy expectations."[111] Not only do people have misunderstandings about privacy notices, but these misunderstandings are systematic and predictable based on people's privacy expectations.

---

106 JOSEPH TUROW, LAUREN FELDMAN & KIMBERLY MELTZER, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005). Another study also found that a majority of people falsely believed that having a privacy policy meant that a site could not share personal data with third parties. *See* JOSEPH TUROW, JENNIFER KING, CHRIS JAY HOOFNAGLE, AMY BLEAKLEY & MICHAEL HENNESSY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 21 tbl.9 (2009) [hereinafter TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT] (finding that 62% think the following statement is true, and 16% "don't know"— "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission").

107 TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT, *supra* note 106, at 20.

108 Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy* Homo Economicus, 49 WAKE FOREST L. REV. 261, 283–84, 302 (2014).

109 *Id.* at 305.

110 Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MKTG. 210, 219 (2015).

111 *Id.* at 220.

E. Inertia and Friction

Another explanation for the privacy paradox is that people generally have inertia when it comes to taking steps to protect their privacy. People hardly ever read privacy notices.[112] They rarely opt out.[113] They often don't change default privacy settings.[114]

As William McGeveran notes, companies that desire people to share personal data aim to create an architecture of "frictionless sharing" to encourage people to share their personal data more readily.[115] McGeveran points out that companies use the term "friction" to describe "forces that impede individuals from disclosing personal information when they use online services, particularly social networks . . . ."[116] Many companies that want people to share more personal data strive to reduce friction.[117] McGeveran argues that regulation should seek to increase friction in order to make people more careful in sharing.[118] He quotes a line that Lawrence Lessig once penned: "Friction is . . . privacy's best friend."[119]

Friction also has a flip side for privacy. Just as readily as friction can discourage people from sharing personal data, it can discourage people from engaging in privacy-protective behaviors. The more cumbersome it becomes to change privacy settings, opt out, and implement other privacy-protective measures, the less likely it is that people will do these things. For example, a study by Susan Athey, Christian Catalini, and Catherine Tucker found that "whenever privacy requires additional effort or comes at the cost of a less smooth user experience, consumers are quick to abandon technology that would offer them

---

112 *See, e.g.*, Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 U. CHI. L. REV. 165, 178 (2011) (discussing a study that revealed that people accessed contract boilerplate terms far less than 1% of the time); George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, J. INTERACTIVE MKTG., Summer 2004, at 15, 20–21 (finding that only 4.5% of respondents to an online survey said they always read website privacy notices and 14.1% frequently read them).

113 *See, e.g.*, Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002) (stating that according to one survey "only 0.5% of banking customers had exercised their opt-out rights").

114 *See, e.g.*, Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363, 373 (Alessandro Acquisti et al. eds., 2008) ("In a study of online social networks, we found that the vast majority of users do not change their default (and very permeable) privacy settings.").

115 William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 15 (2013).

116 *Id.*

117 *See id.* at 15–17.

118 *Id.* at 18–19.

119 *Id.* at 60 (quoting LAWRENCE LESSIG, CODE VERSION 2.0, at 202 (2006)).

greater protection."[120] Friction, then, can become privacy's worst enemy. Companies can intentionally raise the friction for people to exercise privacy-protective choices, resulting in a shift in people's behavior. People's failure to read privacy policies, opt out, and take other small privacy-protective steps might be more the outcome of inertia and friction than the product of their privacy preferences.

***

The behavior distortion argument demonstrates that behavior is extremely malleable and thus offers a compelling case for explaining why behavior is not a reliable metric for people's actual attitudes about privacy. The behavior distortion argument undercuts the behavior valuation argument at its central premise and is therefore the clear victor between the two types of responses to the privacy paradox. But as the remainder of this Article contends, the behavior distortion argument does not go far enough as a response to the privacy paradox.

IV. Paradox Denied: Risk and Context

The behavior distortion argument undermines the behavior valuation argument's contention that behavior is a more reliable metric of people's actual preferences than stated attitudes about privacy. But are people's stated attitudes accurate? The behavior distortion argument recognizes that people's attitudes might be subject to some of the same distorting factors as their behavior. Alessandro Acquisti, along with Laura Brandimarte and George Loewenstein, note that "people are . . . likely to be uncertain about their own privacy preferences" because research "shows that individuals often have little sense of how much they like goods, services, or other people [and] [p]rivacy does not seem to be an exception."[121] Thus, the very notion that people may have *actual* or *true* preferences must be qualified. Whether measured via stated attitudes or behavior, preferences themselves are not static; they are highly contextual, subject to distortion, and malleable.[122]

---

120 Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 18 (MIT Sloan Research Paper No. 5196-17; Stanford Univ. Graduate Sch. of Bus. Research Paper No. 17-14, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916489 [https://perma.cc/T96Y-VSHF].

121 Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Information Age*, *in* Cambridge Handbook of Consumer Privacy, *supra* note 56, at 184, 186.

122 *Id.* at 185.

This Article proposes another way to respond to the privacy paradox, one that takes a radical path: the privacy paradox does not exist and individual preferences should not be the focus for establishing the value of privacy or for determining whether regulation is justified.

Properly understood, the behavior in the privacy paradox studies is about preferences that involve risk assessments in contextual situations. In contrast, people's attitudes about privacy are often stated more generally—applying across different contexts. Thus, there is no inconsistency between behavior and attitudes because they are about very different things.

The behavior valuation argument often ends up making claims about the value of privacy based on privacy paradox studies. These claims are based on a series of improper generalizations from people's behavior. Behavior involves a choice based on risk in a very specific context. In its most narrow formulation, the behavior valuation argument generalizes about people's preferences involving specific personal data to reach conclusions about people's preferences about the same data more broadly across many contexts.[123] The argument often generalizes even further, going beyond the specific pieces of data involved with the behavior to make conclusions about how people value the general type of personal data or even to how people value all personal data.[124] And, the argument frequently does not stop there—it generalizes to how people value their privacy in total.[125] This last generalization is based on a reductive conception of privacy, often viewing people as not caring about their privacy if they share their data with third parties. Privacy involves much more than whether or not to share personal data.

This Part explains that many oft-stated conclusions made about the privacy paradox do not follow from people's behavior. The privacy paradox emerges from conflated issues, unwarranted generalizations, and leaps in logic. When the curtain is finally pulled away from the privacy paradox, we see a surprising revelation—there is no paradox after all.

---

123 *See, e.g.*, Ben-Shahar, *supra* note 61 ("[P]eople seem indifferent to Big Data collection. They share personal information on web platforms, knowing full well that it is collected by websites. . . . Economists have found that people are willing to pay at most a few dollars to prevent their apps from harvesting data . . . .").

124 *See, e.g.*, *id.* ("Most people don't value their New Money currency much and therefore don't mind paying with their data.").

125 *See, e.g.*, *id.* ("The ticklish few—those who are more fussy about their privacy or have things to hide . . . .").

A. Value and Risk

The behavior in the privacy paradox studies is not about the value of privacy; instead, the behavior involves decisions about risk in specific contexts. These contexts often involve particular pieces of personal data disclosed to particular parties with particular expectations of use.[126] People's behavior does not conflict with how much they value privacy. Decisions about risk are different from value. *Risk* involves the potential for harm or loss.[127] *Value* is the overall importance that a person ascribes to something.[128]

There is also a difference between how much a person values her own privacy versus how much a person values privacy in general. A person might not want much personal privacy but could still consider privacy valuable from a societal perspective because of its importance to other people's freedom and well-being. Just because a person doesn't choose privacy for herself doesn't mean that she ascribes no value to the right to privacy. The value of privacy isn't based on one's particular choice in a particular context; privacy's value involves the right to have choices and protections. People can value having the choice even if they choose to trade away their personal data, and people can value others having the right to make the choice for themselves.

The behavior in the privacy paradox studies reveals preferences in specific situations; the behavior doesn't reveal enough to draw accurate conclusions about how individuals value privacy. People's preferences are revealed through certain choices that they make between alternatives, and these choices occur at a specific time and place, in a specific context, and between a specific set of alternatives.[129] The conclusion that can be made from this behavior is that in a particular time and place, in a specific context, people choose one alternative over another. Any broader conclusions often do not logically follow.

The behavior valuation argument often reaches conclusions about how people value privacy based on how readily they share their

---

126 *See supra* Part I.

127 *Risk*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/risk [https://perma.cc/WLH8-XPV2].

128 *Value*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/value [https://perma.cc/EZ2Z-9SX3]; *see also infra* Section V.A.1.

129 Alessandro Acquisti, Leslie John, and George Loewenstein aptly observe that the wrong conclusions are drawn based on how people make decisions about their personal data: "Individuals' decisions about their data are sometimes taken as representing true and final preferences toward protection or revelation of personal data and therefore become an instrument for the assignment of societal resources to privacy issues." Acquisti et al., *supra* note 95, at 269.

personal data. However, a more accurate way to understand the behavior exhibited in the privacy paradox is in terms of risk. The choices people make involve their assessment of risk of harm, not how much they value privacy. Understood in terms of risk, what matters isn't the fact that people share their personal data. Many people don't find sharing their personal data to be inherently harmful, but they are concerned about risk—potential downstream uses or disclosures that could harm them.[130] For example, the study by Sarah Spiekermann, Jens Grossklags, and Bettina Berendt assessed behavior via people's supplying personal data while shopping online.[131] However, providing personal data to an online store doesn't mean that people lack concern over privacy; people might have disclosed because they thought that their data would not be used in harmful ways.

In another study led by Zeynep Tufekci, many participants shared information on their social media profiles about their favorite books, movies, and music, as well as their political views, religion, romantic status, and sexual orientation.[132] However, when it came to phone numbers and addresses, the researchers found an interesting gender disparity: "The odds of a man indicating his phone number were 3 times that of a woman, and the odds of him indicating his address were 1.5 times that of a woman, even after controlling for privacy and audience concerns."[133] These results suggest people are focusing on risk—here, women are likely seeking to avoid the risk of unwanted attention.

In the Tufekci study, to evaluate general online privacy concerns, the participants were asked very broad questions such as "[h]ow concerned are you with online privacy?" or "[h]ow concerned are you that people you do not want to see your profile will see it?"[134] But a person could be concerned about online privacy and not be concerned about whether other people know their favorite movies, books, or music. A person might be concerned about harmful uses of their personal

130 *See, e.g.*, Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/H8DN-GNAH] ("[A] [m]ajority of Americans feel as if they have little control over data collected about them by companies and the government.").

131 Spiekermann et al., *supra* note 1, at 39.

132 Zeynep Tufekci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, 28 Bull. Sci. Tech. & Soc'y 20, 27 (2008).

133 *Id.*

134 *Id.* at 25.

data. When disclosing favorite things and even romantic status and sexual orientation, people might not have perceived a large risk. Ironically, study participants were more protective of less sensitive data such as phone numbers and addresses.[135] In terms of risk, this behavior makes sense; people could more readily imagine potential harm from receiving unwanted contact.

Many of the studies exhibiting the privacy paradox do not show that people are ascribing a low value to privacy. Instead, they show people making decisions involving privacy risks. For example, in the Beresford, Kübler, and Preibusch study, conducted in the European Union ("EU"), the researchers focused on whether people provided their monthly income and date of birth to measure their commitment to privacy.[136] People might not have thought that this data raised any notable risks of harm if shared. People didn't publicly release their data; they provided it to stores.[137] The stores were required to follow the strong privacy protections in the EU, which protects against many privacy risks.[138] Thus, providing data to the stores does not demonstrate that the respondents barely valued privacy. Instead, it likely indicates that the respondents viewed the sharing of the data as low risk in the specific context—that the stores would not use the data in ways that would harm them or that the data would not be publicly disclosed and later used to cause harm.

B. Improper Generalizing from Specific Contexts

When people agree to share their data, they share it in a particular context with particular entities.[139] People have assumptions about what these entities might do with the data. For example, a person

---

135 *Id.* at 27.

136 Beresford et al., *supra* note 29, at 26.

137 *Id.*

138 *See id.* at 27; *see also* Paul M. Schwartz & Daniel J. Solove, *Rethinking Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 881–903 (2014) (comparing the differences between U.S. and E.U. privacy law and noting the relatively stronger regulations in the E.U.).

139 "[P]rivacy should be conceptualized contextually as it is implicated in particular problems." Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1093 (2002); *see also* SOLOVE, *supra* note 10, at 101–70 (outlining a taxonomy of privacy harms based on "four basic groups of harmful activities:" "(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion"); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 2 (2010) ("The framework of contextual integrity provides a rigorous, substantive account of factors determining when people will perceive new information technologies and systems as threats to privacy . . . ."); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155 (2004) (developing "a model of informational privacy in terms of contextual integrity, defined as compatibility with presiding

might be fine providing her address to a retailer for one dollar because she assumes that the retailer will use the address to send catalogs or share it with other similar retailers. She would likely behave quite differently if asked to share her personal data with a stalker or a hate group.

The conclusion that can be drawn from these instances is not that people value privacy at a particular amount or even that people value specific pieces of data at a particular amount. Instead, the main conclusion is that in a particular context when data is provided to a particular entity, a person is assessing the risk of undesirable uses as lower than the particular monetary reward.

Moreover, the fact that people state concerns over their privacy does not mean that they are concerned about each and every instance of personal data disclosure or use. As Kirsten Martin and Helen Nissenbaum aptly observe: "Privacy is not lost, traded off, given away, or violated simply because control over information is ceded or because information is shared or disclosed—only if ceded or disclosed inappropriately."[140] In studies about attitudes, people are often asked to think generally about privacy concerns. These general concerns are stripped of context—there is often no indication to whom the personal data will be disclosed, how it will likely be used, or what ways it might be protected.[141] Sometimes, people are asked broadly if they care about privacy without indicating precisely what types of personal data they are most concerned about and what types of personal data do not pose concern.[142] In contrast, the studies about behavior are performed in a highly contextual manner. The studies nearly all involve specific pieces of personal data, shared in specific ways to specific people or entities or on specific sites. Indeed, as Alessandro Acquisti, Curtis Taylor, and Liad Wagman note, "small changes in contexts and scena-

---

norms of information appropriateness and distribution. Specifically, whether a particular action is determined a violation of privacy is a function of several variables . . .").

140 Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 COLUM. SCI. & TECH. L. REV. 176, 191 (2016).

141 *See, e.g.*, Acquisti & Grossklags, *supra* note 23, at 28 (discussing survey about privacy attitudes featuring questions such as "[d]o you think you have enough privacy in today's society?" and requests for specific pieces of information).

142 *See, e.g.*, CONSUMERS INT'L & INTERNET SOC'Y, THE TRUST OPPORTUNITY: EXPLORING CONSUMERS' ATTITUDES TO THE INTERNET OF THINGS 16–17 (2019), https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf [https://perma.cc/S97D-VB72] (asking only for views on how devices collect data in survey of consumer trust in Internet of Things devices, rather than questions revolving around type of personal data collected).

rios can lead to widely differing conclusions regarding consumers' willingness to pay to protect their data."[143]

Often, stated preferences are not articulated to the same degree of specificity as people's observed behavior. The behavior might appear to be in conflict with a stated preference when, in fact, the inconsistency is due to the false assumption that the stated preference encompasses the risks undertaken by the behavior. There are many privacy issues, and not all might trouble everyone. Some people might be most troubled when a lot of data is gathered about them by large companies. Other people might worry primarily about *government* surveillance and access to their data, but might be relatively unconcerned when companies or marketers gather their data. Some people might strongly object to their data being used to deliver advertisements to them. Other people might not care about ads. When people express concern about privacy, they might have very different things in mind.

Also, it is wrong to reach general conclusions about all types of personal data from situations involving particular types of personal data. People care about certain types of personal data more than others, and the concern over which types varies from person to person. Although many people might not be concerned about keeping their address confidential, for a stalking victim who is attempting to hide from her stalker, the confidentiality of her address could be a matter of life or death. Some people might be very guarded about their income; other people might not be concerned at all. Universal conclusions about all types of personal data do not logically follow from particular transactions involving particular pieces of personal data.

Additionally, great caution should be used even when generalizing from one context to a nearly identical context at a different point in time. Even if the same data and parties are involved and even if the privacy risks are the same, a person's risk assessments could be very different. When evaluating privacy risks in making a particular choice, people often do not consider everything in a detailed calculus. They decide based on what is on the front burner in their mind at one moment in time. The privacy paradox studies are not revealing a set of fixed preferences; they are revealing people's choices based on an assessment of risk in a particular context at a particular time. People don't assess risk with perfect rationality like a machine calculating sta-

143 Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 478 (2016).

tistical odds. People make choices on the fly, in a snap judgment. Thus, broader conclusions about how people would act—even in the same or similar contexts—are dubious because at different points in time, people might make decisions about risk quite differently. These decisions depend upon a myriad of factors: what they are currently thinking about, how long they take to make the decision, how aware they are of certain potential privacy risks, and so on.

C. The Many Dimensions of Privacy

The privacy paradox is often based on misunderstandings of privacy. Frequently, conclusions are drawn from studies that go far beyond what the studies have demonstrated. These studies beg the question of what "privacy" means, frequently equating privacy with secrecy. For example, consider the Beresford, Kübler, and Preibusch study involving participants sharing their monthly income and date of birth with an online store.[144] The study authors concluded: "The experiment demonstrates an unwillingness to pay for privacy as the vast majority of subjects provide their monthly income for a price discount of one Euro."[145] This conclusion, however, is far broader than the experiment's results demonstrate. The experiment merely shows that people are unwilling to pay to conceal their monthly income from a store; this is far narrower than an "unwillingness to pay for privacy,"[146] which presumably means all their personal data and all potential things that could be done with it.

Proponents of the behavior valuation argument conclude from people's disclosure of their personal data that they do not care about the privacy of this data.[147] This conclusion, however, relies on too narrow a conception of privacy—it views privacy as tantamount to secrecy. In *Understanding Privacy*, I argued that "privacy" is not just one thing, but a group of related things.[148] Privacy is not just about keeping secrets.[149] When people want privacy, they do not want to hide away their information from everyone; instead, they want to share it selectively and make sure that it is not used in harmful ways. Privacy is not all-or-nothing—it is about modulating boundaries and controlling data flow.

---

144 *See supra* notes 29–33 and accompanying text.

145 Beresford et al., *supra* note 29, at 26.

146 *Id.*

147 *See supra* Part II.

148 SOLOVE, *supra* note 10, at 9.

149 *Id.* at 21–24.

Thus, the fact that people share personal data does not mean that they do not care about privacy. In today's Information Age, if people really wanted to keep all their information concealed, they would have to live in a shack in the woods. The fact that people share data in an age where it is nearly impossible not to do so has little bearing on the value of privacy. Additionally, privacy has many dimensions, many of which are not alienable when people supply personal data to an organization. Many privacy laws require that organizations must keep personal data secure.[150] Some laws limit usage or sale of consumer personal data.[151] Under a number of laws, people retain the right to access their data, request that the data be deleted, and so on.[152] These rights are not alienable; even after providing the data, people retain these rights. Thus, when people share personal data with organizations, they are not giving up all their privacy. They are providing a license to use or share their data in certain ways, but they retain various privacy rights in that data, and giving away the data does not mean that they are sacrificing all privacy in their data. Instead, they are increasing privacy risks only to a limited extent.

When people provide data to researchers or organizations, they are doing so with certain expectations about use, and these expectations shape their assessment of the privacy risks involved. People generally expect that researchers and organizations will keep their personal data confidential or that they will not use their data in nefari-

---

150 *See, e.g.*, 16 C.F.R. § 314.3(a) (2020) (stating that financial institutions must "develop, implement, and maintain a comprehensive information security program"); 45 C.F.R. § 164.530(c)(1) (2020) (requiring covered entities to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information").

151 *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2020) (mandating that people have a right to opt out of the sale of their personal data to third parties). Several laws restrict secondary use. *See, e.g.*, 15 U.S.C. § 1681b(a) ("[A]ny consumer reporting agency may furnish a consumer report under the following circumstances and no other . . . ."); 15 U.S.C. § 6802(c) (restricting third-party disclosure of non-public information conveyed by a regulated financial institution); 18 U.S.C. § 2710(e) ("A person subject to this section shall destroy personally identifiable information as soon as practicable . . . ."); 47 U.S.C. § 551(e) (mandating when cable operators are to destroy personally identifiable information); General Data Protection Regulation, Council Regulation 2016/679, art. 5(1)(b), 2016 O.J. (L 119) 1, 35 (information must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes").

152 *See* 15 U.S.C. § 1681g(a)(1)–(2) (stating that a consumer has the right to obtain "information in the consumer's file at the time of the request" as well as "sources of the information"); 45 C.F.R. § 164.524(a)(1) (2020) ("[A]n individual has a right of access to inspect and obtain a copy of protected health information . . . ."); 15 U.S.C. § 6502(b)(1)(B) (right of parents to access and delete data about their children); CIV. § 1798.105(a) ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.").

ous ways. When people give their data to others, they are thus not giving it up with the expectation that anything goes concerning how their data is used, maintained, or transferred.[153]

People are essentially making a risk assessment, and the monetary value for the data is really a payment to accept a certain amount of risk—it is not a payment to give up all privacy. In fact, ironically, the existence of privacy protections might lower the monetary value needed for people to share their data because the protections reduce the risk of the data being used in certain problematic ways. In other words, the fact that people trade personal data for a small amount of money does not suggest that there ought to be less privacy regulation; instead, privacy regulation might be lowering the price of the personal data. Even more boldly, perhaps privacy regulation makes people feel comfortable enough to share personal data with organizations or to engage in e-commerce. The existence of privacy regulation might end up facilitating more information flow than it restricts.

***

Time for a pop quiz. If a person shares the name of her favorite book in exchange for a $1 discount from a particular online bookstore, what can be concluded from this behavior?

A. The person values privacy at only $1.

B. The person values her own privacy at only $1.

C. The person values the privacy of her personal data at only $1.

D. The person values the privacy of her favorite book for only $1.

E. The person values the data about her favorite book at only $1.

F. None of the above.

The answer is F. Answer A is wrong because behavior in a particular transaction does not reveal a person's valuation of privacy in general. It involves her assessment of risk in a particular situation. A person can value privacy highly but might not protect her own privacy. To use an analogy, a person could value the right to vote generally but not vote themselves. The fact that they do not vote can be understood by looking at the context—for example, the person might live in a place where the election is not competitive.

Answer B is wrong because the book is just one of many privacy issues, and its disclosure to a store might not be something that poses a concern to the person.

---

153 *See* Martin, *supra* note 110, at 211–12.

Answer C is wrong because the book is just one piece of personal data and says nothing about other pieces of personal data.

Answer D is wrong because it universalizes from one dimension of privacy to all dimensions of privacy. The person provided the information about her favorite book to a store. The person could expect the data to remain confidential, to be kept secure, to be maintained accurately, and so on. Sharing data with another does not mean that a person lacks concern over privacy, as privacy has many dimensions beyond keeping data totally secret.

Finally, Answer E is tempting because it is so narrow, but even this answer is wrong. The person's behavior does not reveal how she values the data about the book. This is because the data is not being shared with the entire world and stripped of all protections. The behavior indicates instead that the person is willing to provide the data to a particular store for $1.

In a different context, the price might be a lot higher. Suppose the person worked for a company, the book was highly critical of that company, and the data was to be shared with the person's boss. The person would likely not share it for just $1. Moreover, providing the data to the store is different from publicly disclosing the data, or providing it to a government spy agency, or selling it to a hacker who might try to use it to guess passwords. The person likely understands that the store operates under legal obligations for protecting the privacy of the data, and the person has an expectation about likely uses of the data. The person might expect that the store will use the data to advertise to her but not to defraud or harm her.

Additionally, when a bookstore asks for a person's favorite book, the person might assess the risk of sharing this information as low because the information seems quite relevant for a bookstore. Moreover, the person's feelings about the particular store can have an impact too—the person might trust a particular store more than other stores and thus be more willing to share personal data. Another store without the same level of trust might have to provide a higher discount for the person to agree to share the data.

So, what can be concluded when a person provides the name of her favorite book to an online bookstore for a $1 discount? In this particular transaction, at one particular time, involving a particular store and a particular piece of data, the person determined that the risk of sharing the data was low enough to undertake for a $1 discount.

The behavior valuation argument, however, rarely makes such narrow conclusions. It leaps to much broader conclusions and creates a conflict with people's attitudes, which are expressed much more generally. This produces an inconsistency. Then, the fancy name of "privacy paradox" is slapped on, and it seems like something profound is going on. In fact, what is really going on is just a failure of logic.

V. Implications for Policy and Regulation

Although the privacy paradox is not a paradox, this does not mean that the behavior exhibited in the above studies should be ignored or dismissed as irrelevant to privacy regulation. People's behavior generally demonstrates that they are failing to protect their own privacy and are readily sharing their personal data. What conclusions about privacy regulation should follow from people's privacy behavior?

This Part makes two broad contentions. First, it critiques the conclusion frequently made by proponents of the behavior valuation argument that the behavior demonstrates that privacy regulation overvalues privacy and should be lessened or curtailed.

Second, this Part explains why counteracting the distortion on behavior will not substantially improve privacy protection. Privacy regulation too often relies on privacy self-management as its major tool for privacy protection. This approach is doomed to fail, and it will not be saved by curing the irrationalities in people's behavior because even totally rational people cannot succeed at privacy self-management. Instead, this Article suggests a different strategy for privacy regulation.

A. Determining the Value of Privacy

The behavior valuation argument concludes that people's behavior demonstrates that privacy regulation overvalues privacy and should be lessened. Regulation should avoid interfering with transactions where people are giving up personal data for goods, services, or discounts because the market has established a price for privacy. As Adam Thierer argues, there is a value exchange when people trade their privacy for online goods and services that "creates substantial benefits for both producers and consumers."[154] Thierer concludes that despite the difficulty, we should seek to ascribe a monetary value to

154 Adam Thierer, *Are Benefit-Cost Analysis and Privacy Protection Efforts Incompatible?*, *in* Cambridge Handbook of Consumer Privacy, *supra* note 56, at 561, 568.

privacy "because we live in a world of limited resources and inescapable trade-offs."[155]

The behavior valuation argument's approach to determining the value of privacy conflates individual valuation with the value of privacy. As this Section argues, the value of privacy is very different from individual valuations of privacy.

1. The Problems with Individual Valuation

Neither attitudes nor behaviors are good metrics for the value of privacy. Looking at attitudes or behaviors involves attempting to arrive at the value of privacy empirically. Privacy's value, however, is not readily determined empirically. One problem with looking at attitudes and behaviors is that they are focused on individuals—what they say and what they do. The behavior valuation argument fails because it seeks to determine the value of privacy for regulation based upon looking at individual valuations of privacy—often determined empirically in monetary terms.[156] When it comes to privacy regulation, however, it is the value of privacy, not individual privacy valuations, that should inform regulatory decisions. Privacy is a constitutive element of a free and democratic society and is valuable because it is instrumental for many important societal ends. The value of privacy and individual valuations of privacy are very different things. Additionally, the value of privacy cannot be meaningfully captured in monetary terms.

Moreover, the value of privacy should not be determined by looking at the average of individual attitudes or the preferences of the majority. Privacy's value is based on its contribution to democracy, individual well-being, social structure, free expression, and belief. Paul Schwartz aptly contends that "privacy is best conceived of as a constitutive element of civil society."[157] Schwartz argues that privacy protections are necessary for "deliberative democracy and an individual capacity for self-determination."[158] As Zeynep Tufekci aptly observes, "[d]ata privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices."[159]

---

155 *Id.* at 561.

156 *See supra* notes 154–55 and accompanying text.

157 Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999).

158 *Id.* at 1658.

159 Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES, (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html [https://perma.cc/JH37-N3FM].

Proponents of the behavior valuation argument often attempt to use calculations of the monetary value of personal data in making arguments about privacy regulation. They point to many instances where people trade personal data for low monetary amounts and use this to argue that the cost of privacy regulation outweighs the monetary value of personal data to individuals.[160]

Attempting to establish a monetary value for privacy not only makes the mistake of focusing on individual valuation, but it worsens the error by attempting to define this individual valuation in monetary terms. Calculating a monetary value for privacy is fraught with error because calculations are based on individual risk decisions in specific contexts, which are not reflective of the value of privacy generally. As Angela Winegar and Cass Sunstein's study involving the dramatic influence of the endowment effect on valuation of personal data concludes, "[t]he divergence between statements of value and actual behaviour, together with imperfect information and the wide variation in monetary valuation depending on seemingly irrelevant contextual features, make it exceedingly difficult to place any kind of monetary value on data privacy."[161]

Calculations of the monetary value of personal data are not only inaccurate, but also irrelevant for crafting privacy regulation. When assessing the value of a product in the marketplace, it makes sense to assess what people are willing to pay for it. Individual assessments of value are useful to determining the general value of the product. But privacy is not a product. Privacy has a value beyond what people will pay for it and beyond how valuable it is to particular individuals. Of course, privacy does not have transcendent value above all else; in particular situations, privacy can be trumped by other conflicting values. But there are other ways to value things beyond money and beyond focusing on individual valuations.

Consider the arguments about monetary value if applied to free speech. Suppose a study revealed that the average person would agree to refrain from criticizing the government for ten dollars. We wouldn't conclude that the value of free speech is ten dollars. Instead, the value of free speech transcends particular transactions. Commentators would likely not talk about a "free speech paradox."

The fact that people trade their privacy for products or services does not mean that these transactions are desirable in their current

160 *See, e.g.*, *supra* note 53 and accompanying text.

161 Winegar & Sunstein, *supra* note 93, at 433 (citation omitted).

form. Of course, privacy regulation should not halt all tradeoffs that people dislike; nor should it forbid all exchanges of personal data for goods or services. But the mere fact that people make a tradeoff does not mean that the tradeoff is fair, legitimate, or justifiable. For example, suppose people could trade away food safety regulation in exchange for cheaper food. There would be a price at which some people would accept greater risks of tainted food. The fact that there is such a price does not mean that the law should allow the transaction.

Regulation has a role to play with privacy because there are problems with transactions involving personal data that the market fails to address. People are often forced into making tradeoffs. In one survey, 81% of respondents said that they had at least once "submitted information online when they wished that they did not have to do so."[162] People often are not afforded much choice or face a choice between two very bad options.

On the internet, people are often presented with a take-it-or-leave-it choice: provide personal data, allow certain uses, and receive access to information, or don't provide personal data, don't use the service, and don't receive access to the information.[163] This set of choices stems from the common business model of the internet—provide free online content and monetize it by collecting, using, or selling personal data. Chris Hoofnagle and Jan Whittington contend that most "free" online services and information are not free: the price is people's data.[164] Even more problematic is the fact that personal information is not like money. Transaction costs and opportunism inure in personal information transactions that can affect the parties long after the initial trade.[165]

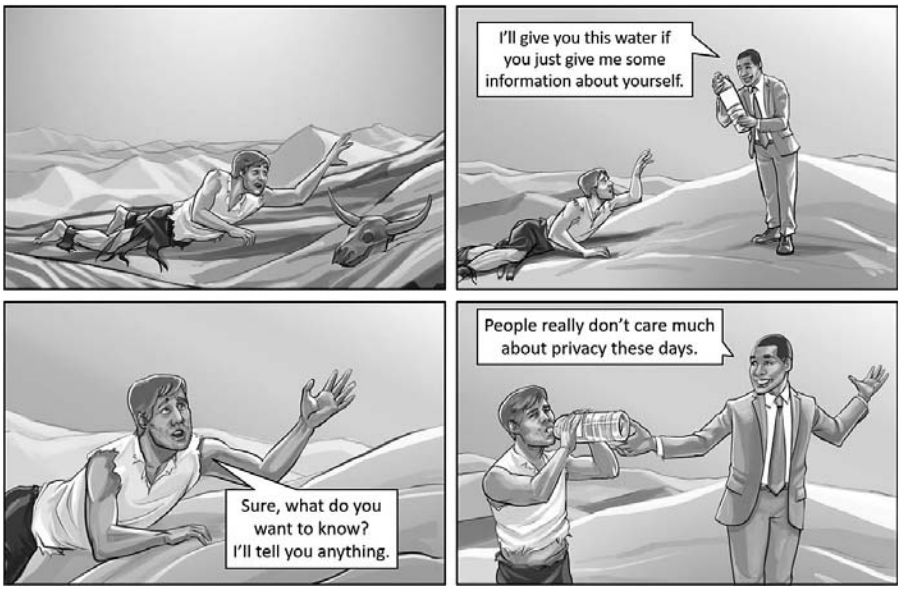
---

162 Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 271 (2016).

163 *See* Frederik J. Zuiderveen Borgesius, Sanne Kruikemeier, Sophie C. Boerman & Natali Helberger, *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation*, 3 EUR. DATA PROT. L. REV. 353, 353 (2017).

164 Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 608–09 (2014).

165 *See id.* at 610–11, 614.



Written by Daniel J. Solove and illustrated by Ryan Beckwith

New technologies are a major fact of our lives. We live in a world where it is becoming increasingly hard to forgo using these technologies, especially when they are very useful and beneficial. People who want to fully protect their privacy must forgo using new products, which are increasingly made with internet connections. They must forgo buying things online, using smart phones, paying with credit cards, and using other basic tools of modern life. To escape from data collection, people must live an isolated and hermetic existence.

Attempts to place a monetary value on personal data are doomed to be completely inaccurate as a metric of anything meaningful. The monetary amount placed on privacy does not reflect privacy's value; at best it reflects a risk assessment, which is infected by behavioral distortions and not able to be performed in a meaningful way due to lack of knowledge or lack of choice.[166] To the extent that people are resigned to not being able to self-manage their privacy, their choice to share personal data for any price is less a reflection of the value of the data and more a reflection of their powerlessness and resignation.

2. Why Is Privacy Valuable?

Privacy's value is not measured by looking at how readily people trade their personal data. There are many reasons why privacy is valuable that transcend individual choices in particular contexts and that

166 *See supra* Part III.

involve providing protection to individuals not just for their own sake but for the larger social good. This Section briefly discusses a few of the most important reasons why privacy is valuable.

Limit on Power. Privacy is a limit on the power of the government and companies. When it comes to personal data, knowledge is power. Personal data is involved in many very important decisions about people's lives. Personal data can readily be used to affect reputations, shape decision-making, and influence behavior. In the wrong hands, personal data can be used to cause great harm to people. People might not be aware of the potential harm when making particular decisions about sharing their personal data, especially when the harm might emerge much later in time.

Respect for Individuals. Respecting a person's privacy is essential for respecting their personhood. It is disrespectful to ignore a person's reasonable desire for privacy without a compelling purpose. Naturally, the desire for privacy can conflict with other key values, and privacy will not always win out. But a person's desire for privacy should at least be considered if one is to respect a person's own judgments about what is in their self-interest. This general respect for people ought to be given even if many people might ultimately choose to trade away their personal data.

Reputation Management. Privacy provides people with the ability to manage their reputations. Reputation affects personal and career opportunities, friendships, and overall well-being. Although complete control over reputations is impossible, it is important that people have the ability to protect their reputations from unfair harm. In addition to protecting people against falsehoods, there are legitimate reasons to also protect people against the disclosure of certain truths. Just because one knows private details about a person does not mean they have a more accurate picture of that person or form a better judgment.[167] Judgments about others are often made in haste, out of context, without the whole story, and with hypocrisy.[168] Privacy thus helps people shield themselves from such judgments. The law in many societies protects reputation not just for the sake of particular individuals, but also because such protection is part of the fabric of civilized society and prevents duels or other social conflict.[169]

---

167 SOLOVE, *supra* note 10, at 144.

168 *See id.* at 144–45.

169 *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 114–17 (2007).

Maintaining Appropriate Social Boundaries. People establish physical and informational boundaries from one another. In order to relax and be less reserved, people need places of solitude and retreat where they can escape the gaze of others.[170] People establish informational boundaries that vary across different relationships. Privacy plays a key role in managing these boundaries. Breaches of these boundaries can damage relationships and create awkward social interactions. Privacy also reduces social friction. Most people don't want everybody to know everything about themselves—hence the phrase "none of your business." And, most people don't want to know everything about others either—hence the phrase "too much information."

Trust. All relationships depend upon trust. A breach of confidentiality is a breach of trust. In relationships with lawyers, doctors, and other professionals, trust is essential for candor. Trust is also essential in our personal and commercial relationships. A breach of trust in one relationship could cause us to lose faith in other relationships. These relationships are worth protecting beyond each particular individual's desire to protect them; these relationships are important for society.

Control Over One's Life. Personal data is a core component of many decisions affecting people's lives, such as whether they receive a loan or a job. The government uses personal data to determine whether people are investigated, searched at the airport, or denied the ability to fly. Indeed, personal data affects nearly all aspects of life. People are helpless if they do not have a say in how their personal data is used or to object to its use when the use could harm them. A core pillar of freedom is autonomy and control over our own lives. Yet, such control is impossible if many decisions are made about people without their awareness or input.[171] People are often asked to make decisions about their personal data without understanding the implications for how that data might be used later in decisions that have an impact on their lives.

Freedom of Thought and Speech. As Neil Richards contends, privacy is essential for intellectual freedom, such as freedom of speech, belief, or consumption of ideas.[172] Watchful eyes over everything we read or watch can have a chilling effect on our exploration or expres-

---

170 *See* SOLOVE, *supra* note 10, at 164–65.

171 *See also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 36–38 (2004) (discussing how Franz Kafka's *The Trial* provides an apt metaphor for a world whereby individuals do not have control over the distribution or use of their personal data).

172 *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 5–6 (2015).

sion of ideas outside the mainstream.[173] Privacy is also key to the protection of communicating unpopular messages. Privacy not only protects fringe activities, but also shelters more conventional activities, such as criticizing friends, family, or colleagues. Furthermore, people may want to explore mainstream ideas or interests that those around them dislike.

Freedom of Social and Political Activities. Privacy is key to protecting our ability to engage politically and associate with others. The freedom of political association often depends upon doing so privately if one chooses.[174] We protect the privacy of voting to ensure that people vote based on their true conscience.[175] The privacy of political activities outside the ballot box is important too.[176] People should be able to form their political beliefs and engage in policy discourse freely without the interference of the watchful gaze or the intrusive ear. The protection of political activity, belief, and discourse is essential for a free and democratic society—it is a social value, not just an individual one.

Ability to Change and Have Second Chances. People change throughout their lives. People need opportunities to have a second chance, move beyond past mistakes, and reinvent themselves. Privacy nurtures this ability by allowing people to grow and mature free of their past actions and decisions. Because we want to encourage growth and improvement in society, it is important that some misdeeds are shielded.

Protection of Intimacy, Bodies, and Sexuality. Danielle Citron points out the importance of what she terms "sexual privacy," which involves "the social norms (behaviors, expectations, and decisions) that govern access to, and information about, individuals' intimate lives."[177] Privacy protects people's bodies, sexuality, gender, and intimate relationships. According to Citron, protecting sexual privacy helps people "manage the boundaries of their intimate lives" and respects "individuals' choices about whom they entrust with their bodies and intimate information."[178] Protecting sexual privacy invasions is es-

---

173 *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) ("Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream.").

174 *See* SOLOVE, *supra* note 10, at 125–26.

175 *See id.*

176 *See id.*

177 Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1874 (2019).

178 *Id.* at 1876.

sential for equality, as privacy invasions occur more frequently and harmfully to women, minorities, and LGBTQ individuals.[179]

Not Having to Explain or Justify Oneself. Privacy matters because people should not always have to justify their thoughts and actions. People do many things which can be misjudged from afar and lead to embarrassment or worse. Constantly having to think about how others will perceive one's actions is a heavy burden that privacy can help alleviate. The freedom from having to justify oneself is a social value as it is a key difference between a free society and a totalitarian one.

***

Privacy has tremendous value as a constituent element of a free and democratic society. By this, I am not arguing that privacy's value is transcendent. To the contrary, privacy is valuable instrumentally for the various individual and social ends that it fosters. The behavior valuation argument ascribes a low value to privacy by improperly generalizing from highly specific contexts. It wrongly equates what people will pay in a transaction with the value of privacy, which are entirely different things. Further, people's decisions about privacy in specific contexts are often made without knowing about the consequences, which often do not occur until much later on.

B. The Impracticality and Futility of Making Privacy Risk Decisions

One policy response to the gap between people's behavior and attitudes about privacy is to endeavor to counter the distortion of people's behavior to align it with their attitudes. For example, Susanne Barth and Menno de Jong argue that "privacy awareness" could "help users to avoid paradoxical behavior."[180] André Deuker recommends "raising privacy awareness on an application-specific level" and "raising knowledge" about how to protect privacy.[181] A study by Maor Weinberger, Dan Bouhnik, and Maayan Zhitomirsky-Geffet found that increasing knowledge of the threats to privacy can "decrease the online privacy paradox behavior."[182] With education, nudges, strategic

---

179 *Id.* at 1890–98.

180 Barth & de Jong, *supra* note 84, at 1051.

181 André Deuker, *Addressing the Privacy Paradox by Expanded Privacy Awareness—The Example of Context-Aware Services*, *in* PRIVACY AND IDENTITY MANAGEMENT FOR LIFE 275, 280 (Michele Bezzi et al. eds., 2010).

182 Maor Weinberger, Dan Bouhnik & Maayan Zhitomirsky-Geffet, *Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior*, 1 OPEN INFO. SCI. 3, 13 (2017).

framing of choices, and other measures, people might improve the way that they protect their own privacy.

Counteracting behavioral distortion, however, will not lead to significantly greater privacy protection. Studies show that even when some of the distorting influences on behavior are countered, the shifts in behavior are not radical.[183] People don't start to staunchly guard their privacy or pay huge premiums for more privacy. For example, a widely-cited 2011 study led by researchers at Carnegie Mellon University concluded that "contrary to the common view that consumers are unlikely to pay for privacy, consumers may be willing to pay a premium for privacy."[184] In the study, people were asked to shop for batteries—a low privacy concern item—and a vibrator—a high privacy concern item.[185] Participants were randomly assigned to three different configurations.[186] One site had no privacy information, another had irrelevant information, and the third had information about privacy protections.[187] People who were given information about privacy protections paid more on the site with privacy information than on the other sites.[188]

The findings, however, do not present an overwhelming refutation of the privacy paradox. The premium paid for privacy was about the same amount for the vibrator as for the batteries.[189] The privacy premium was also quite low. For example, people paid an average of $15.26 for the vibrator on no information sites and $15.88 for it on privacy information sites, a difference of $0.62—just 4%.[190] The study thus demonstrates that making privacy information more visible has only a very modest effect on people's behavior.

Even if behavior can be changed significantly, trying to cure irrational behavior will not lead to a dramatic change in the effectiveness of privacy protection. The rest of this Section explains why.

---

183 Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RSCH. 254 (2011).

184 *Id.* at 266.

185 *Id.* at 260.

186 *Id.* at 261.

187 *Id.*

188 *Id.* at 262–63.

189 *Id.* at 264.

190 *Id.*

1. The Impracticality of Assessing Privacy Risks

In many cases, it is not possible for people to assess privacy risks in a meaningful way. This problem stems from the fact that privacy risks often involve how personal data will be used in the future. People can be informed about immediate uses, but downstream uses far into the future become more difficult to figure out.

Although people may have generalized privacy concerns, they have difficulty translating these concerns to specific situations involving specific pieces of personal data provided to specific entities. People might be generally concerned about their privacy but not realize the precise ways that their personal information will be used when they give it out.

A complicated dimension of assessing privacy risk is understanding how personal data could be analyzed when combined into an extensive digital dossier about a person. People give out bits of data here and there, and each individual disclosure to one particular entity might be relatively innocuous. But when the data is combined, it starts to become a lot more telling about a person's tastes and habits. I call this phenomenon the "aggregation effect."[191] Modern data analytics works via algorithms examining patterns in large quantities of personal data.[192]

The risk assessment becomes much more complicated based on developments in machine learning—known as "artificial intelligence" in popular culture. Information-intensive firms are using data in more surprising ways completely outside of consumer expectations. Through machine learning, firms are discovering subtle relationships among variables that can reveal information about a person in novel ways. For instance, Yilun Wang and Michal Kosinski's research claims to detect sexual preference from merely viewing photographs of subjects.[193] Kosinski also led a study that predicted personality traits from Facebook likes.[194]

It is nearly impossible for people to understand the full implications of providing certain pieces of personal data to certain entities. People might not realize how certain pieces of data, when combined,

---

191 *See* SOLOVE, *supra* note 171, at 44–47.

192 *See id.* at 3–4.

193 Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images*, 114 J. PERSONALITY & SOC. PSYCH. 246, 254 (2018).

194 Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 PNAS 5802, 5802 (2013).

can reveal other facts about themselves that they do not want to share.[195] Even privacy experts might not be able to predict everything that could be revealed when data is aggregated and analyzed because data analytics often reveal insights from data that are surprising to everyone.[196] Michael Froomkin uses the term "privacy myopia" for the people's "systematic inability to correctly value personal data."[197] As he observes, "Even when the long-term consequences are knowable, it may be unreasonably expensive to game out all the possible scenarios. Indeed, it is difficult if not impossible for an ordinary person to stay informed as to the contemporary uses of even innocuous-seeming personal data."[198]

People's decisions to share personal data are thus not just impulsive or irrational. The benefits of sharing personal data are often easy to identify and understand—such as access to interesting information, sharing one's life with one's friends, using new technologies, or receiving money, discounts, or free services. Privacy risks, in contrast, are often vague, abstract, and uncertain. Privacy risks fare poorly when pitted against immediate and concrete benefits that can be more readily understood and evaluated.

2. Futility and Resignation

Although some privacy paradox studies involve decisions about whether to share personal data, other studies reveal that people do not take other steps to protect their privacy, such as opting out, choosing alternative merchants to transact with, reading privacy policies, accessing their personal data, exercising their privacy rights under the law, carefully calibrating one's privacy settings on sites, encrypting their data, and so on. Some of these privacy-protective steps are easy and inexpensive.

---

195 *See* SOLOVE, *supra* note 171, at 44–47.

196 *See, e.g.*, JOHN CHENEY-LIPPOLD, WE ARE DATA: ALGORITHMS AND THE MAKING OF OUR DIGITAL SELVES 55–67 (2017) ("[B]ig data generates measurable types . . . that might be surprising but are treated as nonetheless correct."); CHRISTIAN RUDDER, DATACLYSM: WHO WE ARE WHEN WE THINK NO ONE'S LOOKING (2014) (providing numerous examples of how data leads to surprising conclusions).

197 A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1732, 1735.

198 *Id.* at 1732; *see also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1504 (2000) ("[I]f consumers are plausibly myopic about the value of a datum—focusing on its marginal value rather than its average value, which is difficult to measure—but profilers are not and the data are more valuable in aggregate, then there will be substantial over-disclosure of personal data even when consumers care about their informational privacy.").

The behavior distortion argument seeks to explain this lack of action as irrational—the product of manipulation, skewing, or certain cognitive biases and heuristics. Alternatively, the behavior is explained as based on a lack of knowledge. The implication is that if we can counteract the biases and heuristics, if we can stop the manipulation and skewing, and if we can educate people, then people will change their behavior and make it align better with their attitudes.

Unfortunately, such a conclusion is too optimistic. Resolving these problems will not result in effective privacy protection. Instead, merely adjusting the conditions so that people engage in more steps to protect their privacy will lead to a dead-end for privacy regulation. Although some studies show that people actually engage in more privacy-protective behavior if the conditions are changed, the effect is limited at best.[199] Even if people acted rationally with full knowledge, they could not meaningfully protect their privacy without radically disconnecting from the modern world.

The problem with privacy self-management is that it does not scale.[200] Viewed in isolation, a person not reading a particular company's privacy policy or not opting out might seem irrational given their preferences. But when they must do so on a gigantic scale, across hundreds and even thousands of websites and organizations, the task is overwhelming. When each individual choice or action to protect privacy is viewed in isolation, it appears simple and not onerous. When people fail to take these small steps, they are viewed as not caring about privacy because the steps are so small. But the larger context is missing—there are too many of these little tasks in totality. For example, a study by Aleecia McDonald and Lorrie Cranor concluded that if people were to read every privacy notice relevant to them, it would take about 201 hours per year.[201] Their study focused just on reading privacy notices; privacy self-management also involves countless other tasks, many of which can take much longer than reading a privacy notice.

One rational response is resignation. A person acting rationally could readily conclude that they cannot do enough privacy-protective tasks to make a meaningful difference for their privacy, and it is thus not worth the effort to do many such tasks given the enormity and tediousness of the overall project. Indeed, as a privacy expert, I con-

---

199 *See, e.g.*, *supra* notes 183–90 and accompanying text.

200 *See* Solove, *supra* note 11, at 1888–89.

201 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 565 (2008).

fess that I'm quite resigned. For example, I don't like receiving catalogs in the mail. I used to spend a lot of time and effort trying to opt out, but eventually, I gave up because the catalogs kept multiplying. I didn't have time to keep at it, and it was a losing battle.

In a study, Eszter Hargittai and Alice Marwick interviewed young people about their social media use.[202] The interviewees expressed awareness of many privacy risks associated with disclosing their personal data online, but they felt resigned to their limited control over their data: "[P]articipant comments suggest that users have a sense of apathy or cynicism about online privacy, and specifically believe that privacy violations are inevitable and opting out is not an option."[203]

Christian Hoffmann, Christoph Lutz, and Giulia Ranzini posit that the privacy paradox might be due to what they call "privacy cynicism."[204] They hypothesize that people with weak internet skills will become cynical as a "coping mechanism" in the face of "uncertainty, powerlessness and mistrust" that enables people to "discount risks or concerns without ignoring them."[205] Privacy cynicism is a real phenomenon, and it is not merely a coping mechanism. Privacy self-management is too overwhelming a task to do; even when people try, they cannot learn enough to make informed decisions. Privacy cynicism is perhaps the most rational response of all, no matter how much people know or how adroit they are with technology.

Much privacy regulation attempts to protect privacy by giving people more privacy self-management, which often occurs in the form of granting people more individual rights regarding their personal data, such as a right to opt out of data sharing, a right to notice, a right to delete, and so on.[206] Providing privacy rights is not a bad thing. But if the goal of privacy regulation is to protect people from harms that may arise from collecting, maintaining, using, or disclosing their personal data, then the regulation is failing.

For example, the California Consumer Privacy Act ("CCPA") focuses extensively on privacy self-management.[207] The law gives people

---

202 Eszter Hargittai & Alice Marwick, *"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy*, 10 INT'L J. COMM. 3737, 3741 (2016).

203 *Id.* at 3752.

204 Christian Pieter Hoffmann, Christoph Lutz & Giulia Ranzini, *Privacy Cynicism: A New Approach to the Privacy Paradox*, 10 CYBERPSYCHOLOGY: J. PSYCHOSOCIAL RSCH. ON CYBERSPACE 1 (2016), https://cyberpsychology.eu/article/view/6280 [https://perma.cc/W6PL-Y297].

205 *Id.* at 2, 4.

206 *See supra* notes 150–52 and accompanying text.

207 CAL. CIV. CODE §§ 1798.100–.199 (West 2020).

robust rights to find out about the personal data that companies are gathering about them. People can make a request to a company for information about their personal data, including all the specific pieces of personal information that companies have gathered about them over the past year.[208] The law then mandates that people have a choice to opt out of the sale of that data to third parties.[209]

At first glance, the law appears to give people a lot of control over their personal data—but this control is illusory. First, many companies gather and maintain people's personal data without people knowing.[210] People must know about the companies gathering their data in order to request information about it and opt out. So, the CCPA helps people learn about the data collected by companies they already know about but does not help them learn much about what data is being gathered by other companies that operate in a more clandestine way.

Second, the CCPA does not scale well. The number of organizations gathering people's data is in the thousands.[211] Are people to make thousands of requests? Opt out thousands of times? People can make a few requests for their personal data and opt out a few times, but this will just be like trying to empty the ocean by taking out a few cups of water.

Third, even when people receive the specific pieces of personal data that organizations collect about them, people will not know enough to understand the privacy risks. Journalist Kashmir Hill notes how requests for personal data from companies often involve a data dump, which has limited utility: "[M]ost of these companies are just showing you the data they used to make decisions about you, not how they analyzed that data or what their decision was."[212] A list of pieces of personal data mainly informs people about what data is being col-

---

208 *Id.* § 1798.100(a).

209 *Id.* § 1798.120(a).

210 *See, e.g.*, Sarah Steimer, *The Murky Ethics of Data Gathering in a Post-Cambridge Analytica World*, AM. MKTG. ASS'N (May 1, 2018), https://www.ama.org/marketing-news/the-murky-ethics-of-data-gathering-in-a-post-cambridge-analytica-world/ [https://perma.cc/F2AH-Y37Q] (discussing how the Cambridge Analytica data scandal revealed the myriad of ways Facebook was unknowingly collecting consumer data).

211 Bruce Schneier, *It's Not Just Facebook. Thousands of Companies Are Spying on You*, CNN (Mar. 26, 2018, 8:19 PM), https://www.cnn.com/2018/03/26/opinions/data-company-spying-opinion-schneier/index.html [https://perma.cc/8QRH-4UPB].

212 Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too.*, N.Y. TIMES (Nov. 4, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html [https://perma.cc/ZRG2-W7A3].

lected about them, but privacy risks often involve how that data will be used.

Although the CCPA is well-meaning, it might lull policymakers into a false belief that its privacy self-management provisions are actually effective in protecting privacy. Worse, it might greenlight extensive data selling—after all, under the CCPA, companies are allowed to sell data unless the individual opts out.[213] Policymakers might pat themselves on the back and consider the problem of privacy to be largely solved. Other measures to protect privacy might not be enacted.

Of course, there is risk reduction when one partially manages privacy, but on the whole, the series of tasks involved in managing one's privacy is endless, and many people might not see enough risk reduction in doing a few privacy self-management tasks to be worth the time, effort, or tradeoffs. The problem is that the privacy-protective options that the studies present to people are mostly privacy self-management activities. People can't really do self-management well, even when not encumbered by cognitive influences on their behavior.[214] As the previous Section explained, accurately assessing privacy risks is a daunting—if not impossible—task while managing privacy systematically is futile. Resignation is far from an irrational response. Although people might not consciously and rationally reach the conclusion that most of their efforts to protect privacy are futile, they might still sense it and resign themselves.

Thus, perhaps people's behavior is not so irrational after all. They are just resigned to a world where there is little meaningful action they can take. This conclusion does not mean that people will always throw caution to the wind and post all of their personal data publicly online. Instead, recognition of the futility might make people more inclined to trade personal data for small rewards, use new technologies that carry significant privacy risks, not opt out of data sharing and uses, fail to use the optimal privacy settings, or not request information from companies about the use of their personal data, among other things. Indeed, at some point nearly everyone will reach the limit of how much privacy self-management they can do; some just reach the limit sooner than others.

Meaningful privacy protection cannot rely primarily on privacy self-management. Providing rights to manage privacy can be helpful in

213 CIV § 1798.120(b).

214 Solove, *supra* note 11, at 1888–93.

particular contexts, but an overall strategy to protect privacy will fail if it relies on people doing an almost infinite amount of privacy self-management. People will be given more buttons, switches, tick boxes, and toggles. The result of increasing the amount of privacy self-management is akin to doling out yet more homework, heaping on more tasks that people lack the time or ability to do.[215]

The control that people are being given is illusory. It is not real control, just busy work. When people fail to complete the infinite mountain of tasks, when they give up, or when they don't bother to try, the situation starts to resemble the privacy paradox. Proponents of the behavior valuation argument point to these behaviors and claim that they indicate that people are not very concerned about their privacy.[216] The blame is placed on people for not doing enough to protect their privacy; people might even blame themselves.

The privacy paradox is a myth, born out of this vicious cycle when people express concerns about their privacy, are given a dose of privacy self-management in response, fail to succeed at the impossible project of privacy self-management, and then become disillusioned and resigned. People continue to express privacy concerns—and the cycle keeps repeating. To be effective, privacy regulation must break out of this cycle.

3. Regulating the Architecture of the Personal Data Economy

There is a role for privacy regulation that goes beyond relying heavily on privacy self-management. A significant amount of privacy protection can be accomplished beyond affording people with notices, rights, and choices. Highly effective privacy regulation focuses on the architecture of the personal data economy—data collection, use, storage, and transfer.

For example, one component of this architecture involves regulating the transfer of personal data to third parties. Organizations enter into contracts when transferring and receiving personal data to or from other organizations. For midsize to large organizations, these contracts can number in the hundreds or thousands. The extent to

---

215 *See also* Solove, *supra* note 11, at 1889 ("The problem is reminiscent of the beleaguered student whose professors collectively assign too much reading each night. From the perspective of each professor, the reading is a reasonable amount for an evening. But when five or six simultaneously assign a night's worth of reading, the amount collectively becomes far too much. Thus, even if all companies provided notice and adequate choices, this data management problem would persist . . . .").

216 *See, e.g.*, Goldman, *supra* note 67 ("Consumers may tell survey takers they fear for their privacy, but their behavior belies it.").

which these contracts protect personal data matters significantly. This vast colony of contracts remains largely unseen by consumers, who are not involved in the drafting or negotiation of them. Privacy regulation can regulate the terms of these contracts.

Privacy regulation can also regulate to make certain types of personal data transfers impermissible or more difficult to undertake. Additionally, privacy regulation can control downstream transfers and uses of personal data, protecting the data as it flows from an initial transfer to other organizations down the line.

Internal governance within organizations also matters. The resources and authority of the chief privacy officer—or the data protection officer as referred to in the EU—can have significant effects. Among other things, a powerful governance program involves conducting risk assessments, having privacy experts become involved early on in the design process for new technologies, and ensuring that privacy and ethics are taken into account in organizational decisions.

Privacy regulation can also address the design of products or services by prohibiting designs that could lead to consumer harm or establishing processes which allow designers to better evaluate the risks new technologies pose.

Additionally, regulation can establish boundaries for data collection and use by preventing these activities when they go beyond people's likely expectations or when they are unfair or potentially harmful. Regulation can ensure effective data security and can restrict design that is insecure or that creates unwarranted privacy risks.

The purpose of this Article is not to set forth a detailed recipe for privacy regulation; it is just to point out that there are approaches that go beyond more privacy self-management.

Conclusion

The privacy paradox is not a paradox. A paradox is something that is self-contradictory, often absurd. But people's behaviors and attitudes regarding data privacy do not contradict one another. The behavior in the privacy paradox involves choices about risk in specific contexts. Attitudes involve people's broader valuation of privacy, often across many contexts.

After invoking the privacy paradox, many commentators wrongly conclude that people's behavior demonstrates that people really don't value privacy and that privacy protection thus isn't necessary. The privacy paradox is best interpreted not as an indication of how much people value privacy. Instead, the phenomenon demonstrates behav-

ior involving risk, where many factors might influence people's decisions.

The privacy paradox studies certainly demonstrate that there is a gap between people's attitudes and behavior regarding privacy. In response to this gap, many commentators try to find ways to make attitudes and behavior align. Indeed, on the surface, it seems as though behavior and attitudes about privacy should align. But the gap between privacy behavior and attitudes is not an anomaly that should be rectified; the gap exists because the behavior and attitudes are about different things. The effort to try to align them falters because they cannot be fully aligned.

Commentators seeking to close the gap between attitudes and behavior often see one as true and relatively fixed and the other as false and skewed. But neither attitudes nor behavior are fixed. Nor do attitudes or behavior reflect people's true preferences. Behavior is shaped by context; it does not exist in a pure form outside of a context. Attitudes can be held more abstractly and transcend particular contexts.

As this Article has argued, calling the gap between attitudes and behavior a "paradox" falsely implies that attitudes and behavior are about the same thing and should align. Although attitudes and behavior are related to each other, they are about different things, and thus there is no inconsistency when they fail to align.

The privacy paradox has become privacy lore, for it is constantly mentioned and discussed, and sometimes weaponized to attack privacy regulation. However, the privacy paradox is a myth. It only appears to be a paradox because of conflated issues and flawed logic.