2020

The Myth of the Privacy Paradox

Daniel J. Solove

The Myth of the Privacy Paradox

by

Daniel J. Solove

GW LAW

February 1, 2020

THE MYTH OF THE PRIVACY PARADOX

by Daniel J. Solove[1]

[1] John Marshall Harlan Research Professor of Law, George Washington University Law School.

For very helpful comments on this article, I would like to thank Danielle Citron, Woodrow Hartzog, Chris Hoofnagle, and Paul Schwartz. Thanks to Jasmine Arooni and Shannon Sylvester for research assistance.

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" argues that people's behavior isn't an accurate metric of preferences because behavior is distorted by biases and heuristics, manipulation and skewing, and other factors.

In contrast to both of these camps, Professor Solove argues 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 their own privacy.

The behavior in the privacy paradox studies doesn't 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. It is perfectly rational for people—even without any undue influences on behavior—to fail to make good assessments of privacy risks and to fail to manage their privacy effectively. Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively. Privacy regulation often seeks to give people more privacy self-management, such as the recent California Consumer Privacy Act. Professor Solove argues that giving individuals more tasks for managing their privacy will not provide effective privacy protection. Instead, regulation should employ a different strategy – focus on regulating the architecture that structures the way information is used, maintained, and transferred.

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. People express strong concern about privacy yet fail to take easy and inexpensive steps to protect their privacy. This phenomenon is known as the "privacy paradox."[2]

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 7,000 results.[3] 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.[4] Because people trade their privacy for small rewards, their behavior reveals that they ascribe a low value to their privacy. Proponents of the behavior valuation argument often take a step further; they contend that the privacy paradox suggests that privacy regulation should be weakened, curtailed, or not enacted. 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. Accordingly, regulators should be reluctant to interfere.

On the opposite side, other 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.[5] 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 on behavior so that people make choices

[2] *See infra* Part I.
[3] Search Results from Google on January 12, 2020, https://scholar.google.com/scholar?hl=en&as_sdt=0%2C9&q=%22privacy+paradox%22&btnG=.
[4] *See infra* Part II.
[5] *See infra* Part III.

more in line with their actual preferences.

In this Article, I take a different path. I argue that the privacy paradox isn't a paradox. The privacy paradox doesn't need to be explained because it doesn't 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. In Part I, I discuss the privacy paradox. In Part II, I examine the behavior valuation argument and in Part III, I explore the behavior distortion argument.

In Part IV, I advance my 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 their own 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 as I have argued in previous works, "privacy" involves a plurality of different things that extend far beyond just keeping data secret.[6] A person does not surrender all privacy when sharing data with others. Many privacy protections remain in place. The inconsistency in attitudes and behavior turns out to be just a myopic misunderstanding of privacy.

In Part V, I examine the policy and regulatory implications of the behavior exhibited in the privacy paradox. Although I aim to debunk the privacy paradox, the exhibited behavior is still quite real. People are not taking measures to protect their own privacy and are readily sharing their personal data. What is the import of this behavior on policy and regulation?

I contend 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, I argue that the value of privacy cannot be determined empirically by examining individual valuations of privacy and cannot be reduced to a monetary figure

[6] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

based on specific transactions. Privacy's value is as a constitutive element in society, not a bartered good in the marketplace.

Further, I examine whether privacy regulation should try to counter the distorting influences on behavior to make people behave more rationally to align their actions with their stated preferences. Although minimizing these distorting influences could be helpful to a limited degree, I contend that even greatly reducing the distortion would not lead to significant improvement in 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, I argue, is based on the futility of what I call "privacy self-management."[7] 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. 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 can't 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 example, the recent California Consumer Privacy Act (CCPA) 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.[8] 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, as I contend, doing countless tasks to exercise more control is an endless and impractical task – and the control is often illusory.

Therefore, I recommend taking privacy regulation in different direction. Privacy regulation can be best strengthened by regulating in ways that don't 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.

---

[7] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013).
[8] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.199 (2018).

I. THE PRIVACY PARADOX AND ITS IMPACT

The privacy paradox has been documented by countless scholars and commentators. 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 in 2002 led by Sarah Spiekermann compared participants' privacy preferences to the personal data they disclosed to an anthropomorphic chat bot while shopping online.[9] The researchers originally hypothesized that people who are more concerned about their privacy would be less detailed, forthcoming, and truthful when answering questions. 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."[10] The findings were particularly eye-opening because the "bot questions were designed to include many non-legitimate and unimportant personal questions."[11] Participants also "had to sign that they agreed to the selling of their data to an anonymous entity." 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.[12]

Subsequent studies revealed a similar inconsistency between people's privacy attitudes and behavior. A 2005 study led by Bettina Berent 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."[13] In 2006, a study by economics professor Alessandro Acquisti and computer scientist Ralph Gross found a dichotomy between people's privacy concerns and Facebook use practices: "We detected little or no

---

[9] Sarah Spiekermann, Jens Grossklags, Jens, Bettina Berendt. *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior*, EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce 38 (2002), available at https://www.researchgate.net/publication/2480871_E-privacy_in_2nd_Generation_E-Commerce_Privacy_Preferences_Versus_actual_Behavior.

[10] *Id.* at 8.

[11] *Id.* at 8.

[12] *Id.* at 8.

[13] Bettina Berendt et al., *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, 48 Communications of the ACM at 104 (2005).

relation between participants' reported privacy attitudes and their likelihood of providing certain information, even when controlling, separately, for male and female members."[14]

In 2007, the disconnect between attitudes and behavior was given a name – the "privacy paradox" – from an article called *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*.[15] The name stuck, and has become the common way of referring to the phenomenon.

Privacy paradox studies are now legion. Broadly, the studies reach a few different findings. Some studies demonstrate that despite people expressing concern about privacy, they fail to take easy and inexpensive privacy-protective measures. For example, a study by Alessandro Acquisti and Jens Grossklags revealed that nearly 90% of participants said they were "moderately or very concerned about privacy."[16] When behavior was examined, 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."[17] Of people "who were particularly concerned about credit card fraud and identity theft only 25.9 percent used credit alert features." [18] Of the people who agreed that "privacy should be protected by each individual with the help of technology," a large number didn't 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."[19]

Other studies show that despite people saying that they value privacy highly, they will nevertheless share their personal data with third parties for small amounts of money. For example, in a study conducted in Europe by Alastair Beresford, subjects were asked to purchase a DVD from one of two identical stores.[20] One store sold the DVDs for 1 Euro less than the other, but the cheaper store requested more sensitive data. Both stores requested the subject's name, postal address, and email address. However, the cheaper

[14] Alessandro Acquisti and Ralph Gross. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, PET 2006, https://dataprivacylab.org/dataprivacy/projects/facebook/facebook2.pdf.
[15] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors,* 41 J. Consumer Affairs 100 (2007).
[16] Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality in Individual Decision Making,* IEEE Security & Privacy 24 (Jan/Feb 2005)., http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Alastair R. Beresford, Dorothea Kübler, and Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* 117 Economics Letters 25 (2012). http://ftp.iza.org/dp5017.pdf.

store required date of birth and monthly income whereas the more expensive store required year of birth and favorite color. 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 with the cheaper price but requiring more personal data.[21]

A study by Bernardo Reynolds 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."[22]

A study lead by Susanne Barth 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."[23] 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."[24]

In their study of people's use of Gmail and Facebook, Lior Strahilevitz and Matthew Kugler found results "consistent with the privacy paradox."[25] 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."[26] However, only about 35% 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 $15 per year. Only 3% of respondents would pay more than

[21] *Id.*

[22] Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, and Vassilis Kostakos, *Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours*, Conference Paper, 2011, https://www.researchgate.net/publication/221054832.

[23] Susanne Barth et al, *Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors Among Users with Technical Knowledge, Privacy Awareness, and Financial Resources,* 41 Telematics and Informatics 55 (2019).

[24] *Id.*

[25] Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?* 45 Journal of Legal Studies 569, 578 (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 592.

[26] *Id.* at 578.

$120 per year.[27] 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."[28]

A number of studies demonstrate that people share personal data for low amounts of money. One study found that people provided their online browsing history for 7 Euros ($10).[29] Another study found that people downloading smartphone apps were willing to pay only in the range of about $1 to $4 to avoid revealing to the app developer various types of personal data such as browsing histories, text messages, locations, and contact lists.[30] Grossklags and Acqusiti found that "individuals almost always chose to sell their information and almost never elect[ed] to protect their information even for values as little as $0.25."[31]

Some studies have produced findings that cut against the privacy paradox to at least some degree.[32] 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."[33] 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."[34] In a study by Kirsten Martin, a "trust game experiment shows respondents are less willing to engage with a

[27] *Id.* at 578.
[28] *Id.* at 593.
[29] Juan Pablo Carrascal et al., *Your browsing behavior for a big mac*, Proceedings of the 22nd international conference on World Wide Web - WWW 13 (2013).
[30] Scott Savage & Donald M. Waldman, *The Value of Online Privacy* (2013), at https://ssrn.com/abstract=2341311.
[31] Jens Grossklags & Alessandro Acquisti, *When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information* (June 7, 2007) (unpublished manuscript), available at http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEIS07.pdf.
[32] Spyros Kokolakis cites to more than 10 studies between 2010 and 2019 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 Computers & Society 1, 10-11 (2015).
[33] Eszter Hargittai and Eden Litt, *New Strategies For Employment? Internet Skills and Online Privacy Practices During People's Job Search*. 11 IEEE Security and Privacy 38 (2013), https://doi.org/10.1109/MSP.2013.64.
[34] danah boyd and Eszter Hargittai, *Facebook Privacy Settings: Who Cares?* 15 First Monday (Aug. 2010), https://journals.uic.edu/ojs/index.php/fm/article/view/3086/2589.

partner who violated privacy by utilizing an ad network as compared to one who used privacy preserving advertising – even when financially advantageous to the individual."[35] These studies, however, have not done much to change the prevailing view about the existence of the privacy paradox.

III. 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 don't value privacy very highly.[36]

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."[37] The behavior valuation argument posits that people's revealed preferences are a better indication of their actual preferences than their stated preferences.[38] 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, regulation should focus on behavior. People's revealed preferences indicates that they don't value their privacy very much, that they are not as concerned about privacy as they say they are, and that they are fine with trading their personal data for the rewards that companies are

---

[35] Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms* (working draft), https://ssrn.com//abstract=3349448.

[36] *See .e.g*. L. Gordon Crovitz, *Privacy? We Got Over It.,* Wall St. J., Aug. 25, 2008, http://online.wsj.com/article/SB121962391804567765.html ("[W]hatever we say about how much we value privacy, a close look at our actual behavior suggests we have gotten over it.").

[37] WOLFRAM ELSNER, TORSTEN HEINRICH AND HENNING SCHWARDT, THE MICROECONOMICS OF COMPLEX ECONOMIES: EVOLUTIONARY, INSTITUTIONAL, AND COMPLEXITY PERSPECTIVES §6.4.1 (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 Markanda, and Paulo A.L.D. Nunes, *Introduction To Economic Valuation Methods in* RESEARCH TOOLS IN NATURAL RESOURCE AND ENVIRONMENTAL ECONOMICS 143 (Amit Batabyal & Peter Nijkamp eds. 2011), available at https://www.researchgate.net/publication/300134725_Introduction_to_Economic_Valuation_Methods.

[38] The notion that revealed preferences are a better reflection of people's actual preferences originates in *revealed preference theory,* which was developed by economist Paul Samuelson. *See* Paul A. Samuelson, *A Note on the Pure Theory of Consumers' Behaviour*, 17 ECONOMICA NEW SERIES 61 (1938).

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."[39] 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.[40]

Cooper notes that "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."[41] 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."[42] Thus, Cooper urges the 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."[43]

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."[44] 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

---

[39] James C. Cooper, *Lessons from Antitrust: The Path to a More Coherent Privacy Policy*, U.S. Chamber Foundation Report, Feb. 26. 2017, https://www.uschamberfoundation.org/reports/lessons-antitrust-path-more-coherent-privacy-policy.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] James C. Cooper and Joshua D. Wright, *The Missing Role of Economics in FTC Privacy Policy*, in CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Jules Polonetsky, Evan Selinger & Omer Tene, eds., 2017).

unknown parties."[45] 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 email and social networking platforms."[46] 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." They argue that the "FTC is using its bully pulpit to cajole companies into supplying too much privacy."[47]

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."[48] 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."[49] Ben-Shahar reaches the conclusion that "Americans are nonchalant with respect to aggressive collection of their personal information."[50] 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."[51] Only the "ticklish few—those who are more fussy about their privacy or have things to hide—can change the settings to turn off 'dataveillance' or buy anonymizing services for less than $100 per year."[52] Thus, he concludes, "There is no market failure in the Big Data sector and no proven need for protective regulation."[53]

Professor Eric Goldman points out that "consumers' stated privacy concerns diverge from what consumers do."[54] 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."[55] 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."[56]

---

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] Omri Ben-Shahar, *Privacy Is the New Money, Thanks To Big Data*, Forbes, Apr. 1, 2016.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] Eric Goldman, *The Privacy Hoax,* Forbes (Oct. 14, 2002).
[55] *Id.*
[56] *Id.*

Economics professor Caleb Fuller contends that the privacy paradox is due to the fact that "individuals express greater demands for digital privacy when they are not forced to consider the opportunity cost of that choice."[57] 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."[58] He goes on note 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."[59] Fuller concludes that his study's "results should add a dose of humility to the impulse to regulate digital privacy."[60]

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. 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. 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 study describes the results as "problematic" and "alarming."[61] The authors conclude: "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. "[62]

In this Part, I will explore various explanations for the privacy paradox based on distorting influences on behavior.

---

[57] Caleb S. Fuller, *Is the Market for Digital Privacy a Failure?*, 180 PUBLIC CHOICE 353–353, 371 (2019).
[58] *Id.* at 371.
[59] *Id.* at 371.
[60] *Id.* at 371.
[61] Spiekermann, *E-Privacy in 2nd Generation E-Commerce, supra* note X at 8.
[62] *Id.* at 9.

A. BIASES AND HEURISTICS

Many scholars have attempted to explain the privacy paradox by pointing to 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."[63] Tversky and Kahneman began their careers at Hebrew University of Jerusalem in the psychology department.[64] Starting in the 1970s, their studies demonstrated that people make decisions in irrationally – but in consistent ways. These decision-making problems were due to certain heuristics and biases that distorted people's ability to assess their options in a rational manner. 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. Economics has since embraced Tversky and Kahneman's work, which forms the bedrock of behavioral economics. Kahneman went on to win the Nobel Prize in Economics.[65]

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.[66] For example, Alessandro Acquisti and Jens Grossklags contend that people are limited by "bounded rationality," which involves the difficulty figuring out what to do in complex situations involving costs, benefits, and risks.[67] They also note that people tend to favor immediate gratification; people give up their data and don't consider the long term costs and consequences. This cognitive tendency is often referred to as "hyperbolic discounting."[68]

Another cognitive explanation for why people readily share personal data is that they have an illusory feeling of control. An article by Laura

---

[63] Amos Tversky and Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases,* 185 Science 1124 (1974); DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011).

[64] Cass R. Sunstein and Richard Thaler, *The Two Friends Who Changed How We Think About How We Think,* The New Yorker (Dec. 7, 2016), at https://www.newyorker.com/books/page-turner/the-two-friends-who-changed-how-we-think-about-how-we-think. 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).

[65] *See* Sunstein and Thaler, *The Two Friends.* Tversky didn't win because he had died, and the prize is not awarded posthumously. *See id.*

[66] 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 and Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review,* 34 Telematics and Informatics 1038 (2017).

[67] Alessandro Acquisti and Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, gains, and Hyperbolic Discounting, in* THE ECONOMICS OF INFORMATION SECURITY 9 (Jean Camp and R. Lewis eds. 2004).

[68] Acquisti and Grossklags, *Privacy Attitudes and Privacy Behavior, supra* note X.

Brandimarte, Alessandro Acquisti, and George Lowenstein argues that "more control over the publication of private information makes control over information access and use by others appear less salient, which consequently decreases individuals' privacy concerns, and increases their willingness to publish sensitive information about themselves.[69] In other words, people are more comfortable supplying personal data when they feel in control –even if that control is illusory.[70]

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.[71] As Will Oremus notes, "Study 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."[72]

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 don't possess it but have the opportunity to obtain it. 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."[73] Winegar and Sunstein note that this is an "unusually large disparity" and a "kind of superendowment effect."[74]

A study led by Alessandro Acquisti found that "endowment effects powerfully influence individual privacy valuations."[75] The researchers

---

[69] Laura Brandimarte, Alessandro Acquisti, and George F. Loewenstein, *Misplaced Confidences Privacy and the Control Paradox*, 4 Social Psychological and Personality Science, 340 (2013), https://ssrn.com/abstract=3305325.

[70] Woodrow Hartzog contends that much of the controls provided on sites is "illusory." Woodrow Hartzog, *The Case Against Idealising Control*, 4 European Data Protection Law Review 423, 426 (2018).

[71] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, Alessandro Acquisti , *Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators,* CHI '09: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 319 (2009).
http://www.guanotronic.com/~serge/papers/chi09a.pdf.

[72] Will Oremus, *How Much Is Your Privacy Really Worth? No one knows. And it might be time to stop asking,* OneZero (Sep 17, 2019), https://onezero.medium.com/how-much-is-your-privacy-really-worth-421796dd9220.

[73] Angela G. Winegar and Cass R. Sunstein, *How Much Is Data Privacy Worth? A Preliminary Investigation*, 42 Journal of Consumer Policy (2019), https://ssrn.com/abstract=3413277.

[74] *Id.*

[75] Acquisti, Alessandro, Leslie K. John, and George Loewenstein., *What Is Privacy Worth?*

noted: "The answers to questions such as 'What is privacy worth?' and 'Do people really care for privacy?' depend not just on whom, but *how*, you ask."[76] The study also revealed significant effects based on the ordering of choices.[77]

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."[78]

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."[79] Hartzog notes that design "affects how something is perceived, functions, and is used."[80] 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.[81]

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."[82] Computer scientist Arunesh Mathur 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."[83]

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

42 Journal of Legal Studies 249 (2013).
[76] *Id.*
[77] *Id.*
[78] SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 83 (2011).
[79] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2019).
[80] *Id.* at 21.
[81] *Id.* at 23.
[82] Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox,"* 31 Current Issus in Psychology (forthcoming 2020). https://ssrn.com/abstract=3456155.
[83] Arunesh Mathur et al, *Dark Patters at Scale: Findings from a Crawl of 11K Shopping Websites,* 3 ACM Hum.-Comput. Interact., No. CSCW, Article 81. (2019).

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 don't see hundreds of faces staring at them. Seeing all those people makes the consequences of speaking more visceral in the immediate moment – much more than just seeing a computer screen. People also say things online that they'd never say to another person face-to-face.

Ultimately, whether design is created deliberately to manipulate us or unwittingly skews 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 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.[84]

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, 75% of people incorrectly believed that the when "a website has a privacy policy, it means the site will not share [their] information with other websites or companies."[85] In another study, also led by Turow, people correctly answered only 30% of questions regarding their privacy online.[86]

Ignorance of privacy rules can even explain popular conceptions of

[84] Jay P. Kesan, Carol Hayes, and Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*,91 Indiana L.J. 267 (2016).

[85] Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun. 1, 2005. Another study also found that a majority of people falsely believed that having a privacy policy meant that a site couldn't share personal data with third parties. *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (September 29, 2009), available at SSRN: http://ssrn.com/abstract=1478214 (finding that that 62% think this 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.").

[86] Joseph Turow et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* 20–21 (Sept. 29, 2009) (unpublished manuscript), *available at* http://ssrn.com/paper=1478214.

consumer privacy behavior. For instance, in their article discussing Alan Westin's theory of privacy, Chris Hoofnagle and Jennifer Urban show that that people that Westin categorized as privacy "unconcerned" or privacy "pragmatist" were more ignorant of actual privacy rules and regulations and tended to falsely believe that protections were in place than people Westin categorized as privacy "fundamentalists." 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.[87]

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."[88] 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."[89] Not only do people have misunderstandings about privacy notices, but these misunderstandings are systematic and predictable based on people's privacy expectations.

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.[90] They rarely opt out.[91] They often don't change default privacy settings.[92]

---

[87] Chris Jay Hoofnagle and Jennifer M Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev 261 (2014).

[88] 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 Journal of Public Policy & Marketing (2015), at p. 25. https://www.researchgate.net/publication/275407645_Privacy_Notices_as_Tabula_Rasa_An_empirical_investigation_into_how_complying_with_a_privacy_notice_is_related_to_meeting_privacy_expectations_online_1

[89] *Id.* at 26.

[90] 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*, 18 J. INTERACTIVE MARKETING 15, 20–21 (2004) (finding that only 4.5% of respondents said they always read website privacy notices and 14.1% frequently read them).

[91] *See* 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").

[92] *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY 363, 369 (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis & Sabrina De Capitani di Vimercati eds., 2008).

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.[93] 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."[94] Many companies that want people to share more personal data strive to reduce friction. McGeveran argues that regulation should seek to increase friction to make people more careful in sharing. He quotes a line that Lawrence Lessig once penned: "Friction is . . . privacy's best friend."[95]

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, in a study led by Susan Athey, the researchers found that "whenever privacy requires additional effort or comes at the cost of a less smooth user experience, participants are quick to abandon technology that would offer them greater protection."[96] 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 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 therefore is the clear victor between the two types of responses to the privacy paradox. But as I contend in the remainder of this Article, the behavior distortion argument does not go far enough as a response to the privacy paradox.

---

[93] William McGeveran, *The Law of Friction*, U. Chicago Legal Forum Vol. (2013), Article 3, at 15, https://chicagounbound.uchicago.edu/uclf/vol2013/iss1/3.

[94] *Id.* at 15.

[95] LAWRENCE LESSIG, CODE VERSION 2.0 202 (2006)

[96] Carleton Athey, Susan and Catalini, Christian and Tucker, Catherine E., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, MIT Sloan Research Paper No. 5196-17; Stanford University Graduate School of Business Research Paper No. 17-14 (April 8, 2018).

IV. PARADOX DENIED: RISK AND CONTEXT

The behavior distortion argument undermines the behavior valuation argument's contention that behavior is more reliable a 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 also be subject to some of the same distorting factors as their behavior. Acquisti, along with Laura Branimarte and George Lowenstein, 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."[97] 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.

I propose another way to respond to the privacy paradox, one that takes a radical path. I contend that the privacy paradox doesn't exist and that 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 the specific personal data to reach conclusions about people's preferences about the same data more broadly across many contexts. 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. And, the argument frequently doesn't stop there: It generalizes to how people value their privacy in total. 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

[97] Alessandro Acquisti, Laura Branimarte, and George Lowenstein, *Privacy and Human Behavior in the Information Age, in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 184, 186 (Jules Polonetsky, Evan Selinger & Omer Tene, eds., 2017).

data.

In this Part, I explain 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.

A. VALUE AND RISK

The behavior in the privacy paradox studies isn't 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. People's behavior doesn't conflict with how much they value privacy. Decisions about risk are different from value. *Risk* involves the potential for harm or loss. *Value* is the overall importance that a person ascribes to something.

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.[98] 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.

[98] Alessandro Acquisti, Leslie John, and George Lowenstein 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 towards protection or revelation of personal data, and therefore become an instrument for the assignment of societal resources to privacy issues." Alessandro Acquisti, Leslie K. John, and George Loewenstein, *What Is Privacy Worth?* 42 Journal of Legal Studies 249 (2013).

The behavior valuation argument often reaches conclusions about how people value privacy based on how readily they share their personal data. However, a more accurate way to understand the behavior exhibited in the privacy paradox is in terms of risk. The choices people are making involves 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 risks – potential downstream uses or disclosures that could harm them. For example, the study led by Sarah Spiekermann assessed behavior via people's supplying personal data while shopping online.[99] 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 Tufckci, many participants shared on their social media profiles information about their favorite books, movies, and music as well as their political views, religion, romantic status, and sexual orientation.[100] 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."[101] These results suggest people are focusing on risk; females likely are seeking to avoid the risk of unwanted attention.

In the Tufckci study, to gauge general online privacy concerns, the participants were asked very broad questions such as "How concerned are you with online privacy?" or "How concerned are you that people you do not want to see your profile will see it?"[102] 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 data. When disclosing favorite things and even romantic status and sexual orientation, people might not have perceived a large risk. Ironically, people were more protective of less sensitive data such as phone numbers and addresses. 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

[99] Spiekermann et al, *supra* note X.

[100] Zeynep Tufckci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites,* 28 Bulletin of Science, Technology & Society 20 (2008).

[101] *Id.*

[102] *Id.*

decisions involving privacy risks. For example, in the Beresford study, conducted in the EU, the researchers focused on whether people provided their monthly income and date of birth to measure their commitment to privacy.[103] 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. The stores were required to follow the EU's strong privacy regulation, which protects against many privacy risks. Thus, providing data to the stores doesn't demonstrate that the respondents barely valued privacy. Instead, it 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.[104] People have assumptions about what these entities might do with the data. For example, a person might be fine providing her address to a retailer for $1 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 doesn't 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 isshared or disclosed—only if ceded or disclosed inappropriately."[105] In studies about

[103] Alastair R. Beresford, Dorothea Kübler, and Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* 117 Economics Letters 25 (2012). http://ftp.iza.org/dp5017.pdf.

[104] "[P]rivacy should be conceptualized contextually as it is implicated in particular problems." Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087, 1093 (2002); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash.L. Rev. 119 (2004).

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

attitudes, people are often asked to think generally about privacy concerns. These general concerns are stripped of context – there is often no indication of to whom the personal data will be disclosed, how it will likely be used, or what ways it might be protected. 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. 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 scenarios can lead to widely differing conclusions regarding consumers' willingness to pay to protect their data."[106]

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 being 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

[106] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy,* 54 J. Economic Literature 442, 478 (2016).

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 statistical 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 also 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 study involving people sharing their monthly income and date of birth with an online store. The study authors conclude: "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."[107] 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 more narrow than an "unwillingness to pay for privacy," 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 don't care about the privacy of this data. This conclusion, however, relies on too narrow a conception of privacy – it views privacy as tantamount to secrecy. In *Understanding Privacy*, I have argued that "privacy" is not just one thing, but a group of related things.[108] Privacy, however, isn't just about keeping secrets. When people want privacy, they don't want to hide away their information from everyone; instead, they want to share it selectively and make sure that it isn't used in harmful ways. Privacy isn't all-or-nothing – it's about modulating boundaries and controlling data flow.

Thus, the fact that people share personal data doesn't mean that they don't

[107] Alastair R. Beresford, Dorothea Kübler, and Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* 117 Economics Letters 25 (2012). http://ftp.iza.org/dp5017.pdf.
[108] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

care about privacy. In today's Information Age, if people really wanted to keep all their information concealed, they'd 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.[109] Some laws limit usage or sale of consumer personal data.[110] Under a number of laws, people retain the right to access their data, request that the data be deleted, and so on.[111] These rights aren't 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. Therefore, giving away the data doesn't mean that they are sacrificing all privacy in their data. Instead, they are increasing privacy risks to some 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 nefarious ways. When people give their data to others, they are thus not giving it up with the expectation that anything goes with regard to how their data is used, maintained, or transferred.

---

[109] *See* Gramm–Leach–Bliley Act (GLBA) Safeguards Rule, 16 C.F.R. § 314.3(a) (financial institutions must "develop, implement and maintain a comprehensive information security program"); Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 C.F.R. § 164.530(c)(1) (requiring covered entities to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information").

[110] *See* California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.199 (2018) (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* Fair Credit Reporting Act, 15 U.S.C. § 1681b; Gramm–Leach–Bliley Act, 15 U.S.C. § 6802(c); Video Privacy Protection Act, 18 U.S.C. § 2710(e); Cable Communications Policy Act, 47 U.S.C. § 551(e); General Data Protection Regulation (GDPR) Article 51(1)(b) (information must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes").

[111] *See* Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681g (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"); Health Insurance Portability and Accountability Act (HIPAA) Regulation, 45 C.F.R. § 164.524(a)(1) ("an individual has a right of access to inspect and obtain a copy of protected health information"); Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6502(b)(1)(A) (right to access and delete data); California Consumer Privacy Act of 2018, § 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.")

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 isn't 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 doesn't suggest that there ought to be less privacy regulation; instead, privacy regulation might be a factor in lowering the price of the personal data. Even more boldly, perhaps privacy norms make 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 don't vote can be understood by looking at the context – for example, the person might live in a place where the election isn't 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.

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 doesn't mean that a person lacks concern over

privacy, as privacy has many dimensions beyond keeping data totally secret.

Finally, E is a tempting answer because it is so narrow, but even this answer is wrong. The person's behavior doesn't reveal how the person values the data about the book. This is because the data isn't just being shared with the entire world and stripped of all protections. The behavior indicates 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 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 the person but not to defraud or harm her.

Additionally, the fact that this is a bookstore might make the person assess the risk of sharing the name of her favorite book as lower because the disclosure seems quite relevant for a bookstore to want to know. 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? The conclusion that can be drawn is that 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 I contend that the privacy paradox isn't a paradox, this doesn't mean that the behavior exhibited in the 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?

In this Part, I make two broad contentions. First, I critique 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, I explain 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 can't succeed at privacy self-management. Instead, I suggest 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 to for online goods and services that "creates substantial benefits for both producers and consumers."[112] Theirer notes argues that despite the difficulty, we should seek to ascribe a monetary value to privacy "because we live in a world of limited resources and inescapable trade-offs."[113]

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

[112] Adam Thierer, *Are Benefit-Cost Analysis and Privacy Protection Efforts Incompatible? in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 561, 561 (Jules Polonetsky, Evan Selinger & Omer Tene, eds., 2017).
[113] Thierer, *supra* note X, at 561.

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. 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."[114] Schwartz argues that privacy protections are necessary for "deliberative democracy and an individual capacity for self-determination."[115] As Zeynep Tufecki aptly observes: "Data 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."[116]

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.

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 Winegar and Sunstein's study involving the dramatic influence of the endowment effect

[114] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1607, 1613 (1999).
[115] Schwartz, *Privacy and Democracy, supra* note X, at 1670.
[116] Zeynep Tufecki, *The Latest Privacy Debacle,* N.Y. Times (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html.

on valuation of personal data concludes: "The divergence between statements of value and actual behavior, 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.[117]
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 isn't 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 doesn't 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 $10. We wouldn't conclude that the value of free speech is $10. 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 meant that these transactions are desirable in their current 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 doesn't 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 doesn't 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."[118] 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:

---

[117] Angela G. Winegar and Cass R. Sunstein, *How Much Is Data Privacy Worth? A Preliminary Investigation*, 42 Journal of Consumer Policy (2019) (citation omitted), https://ssrn.com/abstract=3413277.
[118] Jay P. Kesan, Carol Hayes, and Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*,91 Indiana L.J. 267, 271 (2016).

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. 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.[119] 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.[120]

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 protect their privacy must forgo using new products, which are increasingly made with Internet connections. They must forgo buying things online, using smart phones, using credit cards, and other basic tools of modern life. To escape from data collection, people must live an insolated 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 doesn't reflect privacy's value; at best it reflects a

[119] Chris Jay Hoofnagle and Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 606 (2014).
[120] Chris Jay Hoofnagle and Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 610 (2014).

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. To the extent to which 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?

Why is privacy valuable? There are many reasons why privacy is valuable that involve the type of society we want to live in. These reasons demonstrate that privacy's value isn't measured by looking at how readily people trade their personal data. Below, I will briefly discuss 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. The more someone knows about us, the more power they can have over us. Personal data is used to make very important decisions in our lives. Personal data can be used to affect our reputations; and it can be used to influence our decisions and shape our behavior. It can be used as a tool to exercise control over us. And, in the wrong hands, personal data can be used to cause us great harm.

Respect for Individuals. Privacy is about respecting individuals. If a person has a reasonable desire to keep something private, it is disrespectful to ignore that person's wishes without a compelling reason to do so. Of course, the desire for privacy can conflict with important values, so privacy may not always win out in the balance. Sometimes people's desires for privacy are brushed aside because of a view that the harm in doing so is trivial. Even if this doesn't cause major injury, it demonstrates a lack of respect for that person. In a sense it is saying: "I care about my interests, but I don't care about yours."

Reputation Management. Privacy enables people to manage their reputations. How we are judged by others affects our opportunities, friendships, and overall well-being. Although we can't have complete control over our reputations, we must have some ability to protect our reputations from being unfairly harmed. Protecting reputation depends on protecting against not only falsehoods but also certain truths. Knowing private details about people's lives doesn't necessarily lead to more accurate judgment about people. People judge other people poorly, they judge in haste, they judge out of context, they judge without hearing the whole story, and they judge with hypocrisy. Privacy helps people protect themselves from these troublesome judgments.

Maintaining Appropriate Social Boundaries. People establish boundaries from others in society. These boundaries are both physical and

informational. We need places of solitude to retreat to, places where we are free of the gaze of others in order to relax and feel at ease. We also establish informational boundaries, and we have an elaborate set of these boundaries for the many different relationships we have. Privacy helps people manage these boundaries. Breaches of these boundaries can create awkward social situations and damage our relationships. Privacy is also helpful to reduce the social friction we encounter in life. Most people don't want everybody to know everything about them – hence the phrase "none of your business." And sometimes we don't want to know everything about other people — hence the phrase "too much information."

Trust. In relationships, whether personal, professional, governmental, or commercial, we depend upon trusting the other party. Breaches of confidentiality are breaches of that trust. In professional relationships such as our relationships with doctors and lawyers, this trust is key to maintaining candor in the relationship. Likewise, we trust other people we interact with as well as the companies we do business with. When trust is breached in one relationship, that could make us more reluctant to trust in other relationships.

Control Over One's Life. Personal data is essential to so many decisions made about us, from whether we get a loan, a license or a job to our personal and professional reputations. Personal data is used to determine whether we are investigated by the government, searched at the airport, or denied the ability to fly. Indeed, personal data affects nearly everything, including what messages and content we see on the Internet. Without knowledge of what data is being used, how it is being used, or the ability to correct and amend it, we are virtually helpless in today's world. Moreover, we are helpless without the ability to have a say in how our data is used or the ability to object and express legitimate grievances when data uses can harm us. One of the hallmarks of freedom is having autonomy and control over our lives, and we can't have that if so many important decisions about us are being made in secret without our awareness or participation.

Freedom of Thought and Speech. As Neil Richards contends, privacy is essential for intellectual freedom, such as freedom of speech, belief, and consumption of ideas.[121] Watchful eyes over everything we read or watch can have a chilling effect on our exploration or expression of ideas outside the mainstream.[122] Privacy is also key to the protection of communicating unpopular messages. And, privacy doesn't just protect fringe activities. We may want to criticize people we know to those we know personally yet not share that criticism with the world. A person might want to explore ideas

[121] *See* NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015).

[122] *See* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373 (2000) ("[P]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream.").

that their family, friends, or colleagues dislike.

Freedom of Social and Political Activities. Privacy helps protect our ability to associate with other people and engage in political activity. A key component of freedom of political association is the ability to do so with privacy if one chooses. We protect privacy at the ballot because of the concern that failing to do so would chill people voting their true conscience. Privacy of the associations and activities that lead up to going to the voting booth matters as well, because this is how we form and discuss our political beliefs. The watchful eye can disrupt and unduly influence these activities.

Ability to Change and Have Second Chances. Many people are not static; they change and grow throughout their lives. There is a great value in the ability to have a second chance, to be able to move beyond a mistake, to be able to reinvent oneself. Privacy nurtures this ability. It allows people to grow and mature without being shackled by all the foolish things they might have done in the past. Certainly, not all misdeeds should be shielded, but some should be, because we want to encourage and facilitate growth and improvement.

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."[123] 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."[124] Protecting sexual privacy invasions is essential for equality, as privacy invasions occur more frequently and harmfully to women, minorities, and LGBTQ individuals.[125]

Not Having to Explain or Justify Oneself. An important reason why privacy matters is not having to explain or justify oneself. We may do a lot of things which, if judged from afar by others lacking complete knowledge or understanding, may seem odd or embarrassing or worse. It can be a heavy burden if we constantly have to wonder how everything we do will be perceived by others and have to be at the ready to explain.

* * *

Privacy has tremendous value as a constituent element of a free and democratic society. By this, I am not arguing that privacy is a fundamental right or that its value transcendent. To the contrary, privacy is valuable instrumentally for the various individual and social ends that it fosters. The

[123] Danielle Keats Citron, *Sexual Privacy,* 128 Yale L.J. 1870. 1874 (2019).
[124] *Id.* at 1876.
[125] *Id.* at 1890-97.

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.

B. THE IMPRACTICALITY AND FUTILITY OF MAKING PRIVACY RISK DECISIONS

Another policy response to people's behavior 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."[126] André Deuker recommends "raising privacy awareness on the application-specific level" and "raising knowledge" about how to protect privacy."[127] A study by Maor Weinberger found that increasing knowledge of the threats to privacy can "decrease the online privacy paradox behavior."[128] With education, nudges, strategic 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 aren't radical.[129] People don't start staunchly guarding their privacy or paying huge premiums for more privacy. For example, a widely-cited 2011 study lead by Janice Tsai 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."[130] In the study, people were asked to shop for batteries (low privacy concern) and a vibrator (high privacy concern). Participants could choose from three different online stores to buy these items. One site had no privacy information, another had irrelevant information, and the third had information about privacy protections.[131] People paid more on the site with privacy information than on the other sites.

---

[126] Susanne Barth and Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review,* 34 Telematics and Informatics 1038 (2017).

[127] André Deuker. *Addressing the Privacy Paradox by Expanded Privacy Awareness - The Example of Context-Aware Services*. 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School (PRIMELIFE), Sep 2009, Nice, France. pp.275-283, https://hal.inria.fr/hal-01061063/document.

[128] Maor Weinberger*, Dan Bouhnik, Maayan Zhitomirsky-Geffet, Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior, 1 Open Information Science 3, 13 (2017).

[129] Janice Tsai, Serge Egelman, Laurie Cranor, and Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 Information Systems Research 234 (2011).

[130] *Id.*

[131] *Id.*

The findings do not present an overwhelming refutation of the privacy paradox. Although people "indicated that they had more privacy concerns when purchasing the vibrator as compared to the batteries, their purchasing patterns did not reflect their concerns."[132] The premium paid for privacy was about the same amount for the vibrator as for the batteries.[133] 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%. 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. In the rest of this section, I explain why as well as explore the implications of this claim.

1. The Impracticality of Assessing Privacy Risks

In many cases, it isn't 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."[134] Modern data analytics works via algorithms examining patterns in large quantities of personal data.

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

[132] *Id.* at 18.
[133] *Id.* at 16.
[134] DANIEL J. SOLOVE, THE DIGITAL PERSON 44-47 (2004).

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.[135] Kosinski also led a study that predicted personality traits from Facebook likes.[136]

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, can reveal other facts about themselves that they do not want to share.[137] Even privacy experts will not be able to predict everything that could be revealed when data is aggregated and analyzed, because data analytics are often revealing insights from data that are surprising to everyone.[138]

Thus, people's decisions to share personal data are 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 don't 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 cheap to do.

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 lack of knowledge. The implication is that if we can counteract the biases

---

[135] Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate than Humans At Detecting Sexual Orientation from Facial Images* (2017) available at https://psyarxiv.com/hv28a/.

[136] Michal Kosinski, David Stillwell, and Thore Graepel*, Private Traits And Attributes Are Predictable From Digital Records Of Human Behavior,* 110 PNAS 5802 (Apr. 9, 2013), https://doi.org/10.1073/pnas.1218772110.

[137] SOLOVE, DIGITAL PERSON, *supra note* X, at 44-47.

[138] *See* JOHN CHENEY-LIPPOLD, WE ARE DATA: ALGORITHMS AND THE MAKING OF OUR DIGITAL SELVES (2017); CHRISTIAN RUDDER, DATACLYSM (2014).

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.[139] I contend that 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 doesn't scale. Viewed in isolation, a person's not reading a particular company's privacy policy or not opting out might seem irrational given her preferences. But when she 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 as 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 a year.[140] 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 she can't do enough privacy-protective tasks to make a meaningful difference for her privacy, and thus it is not worth the effort to do many such tasks given the enormity and tediousness of the overall project. Indeed, as a privacy expert, I confess 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. 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

[139] Tsai et al., *supra* note X.
[140] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S, A Journal of Law and Policy for the Information Society 540, 565 (2008).

online privacy, and specifically believe that privacy violations are inevitable and opting out is not an option."[141]

Christian Hoffmann, Christoph Lutz, and Giulia Ranzini posit that the privacy paradox might be due to what they call "privacy cynicism."[142] 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."[143] Although I agree with the existence of privacy cynicism, I contend that it is not merely a coping mechanism. Privacy self-management is too overwhelming a task to do; even when people try, they can't 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.

Providing privacy rights isn't 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 new California Consumer Privacy Act (CCPA) of 2018 focuses extensively on privacy self-management.[144] The law gives people 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. The law then mandates that people have a choice to opt out of the sale of that data to third parties.

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. 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 doesn't help them

[141] Eszter Hargittai and Alice Marwick, *"What Can I Really Do?": Explaining the Privacy Paradox with Online Apathy*, 10 Int'l J. of Communication (Jan. 2016).
[142] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini, *Privacy Cynicism: A New Approach to the Privacy Paradox,* 10 Cyberpsychology: Journal of Psychosocial Research on Cyberspace (2016).
[143] *Id.*
[144] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.199 (2018).

learn much about what data is being gathered by other companies that operate in a more clandestine way.

Second, the CCPA doesn't scale well. The number of organizations gathering people's data is in the thousands. Are people to make 1,000 or more 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."[145] A list of pieces of personal data mainly informs people about what data is being collected about them; but privacy risks often involved how that data will be used.

My concern about the CCPA is that although it 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. 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. As I explained in the previous section, 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 isn't so irrational after all. They are just resigned to a world where there's little meaningful action they can take.

[145] Kashmir Hill, "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too," N.Y. TIMES (Nov. 4, 2019).

This conclusion doesn't 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 particular contexts, but an overall strategy to protect privacy will fail if replying on people doing an almost infinite amount of privacy self-management. People will get more forms to request information about data collected about them. They will be given more buttons, switches, tick boxes, and toggles. With hearty idealism about empowering people, proponents of privacy regulation aim to give people more control over their personal data, but the result is often doling out more homework for people, heaping on more tasks that people lack the time or ability to do.

The control that people are being given is illusory. It's 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. The behavior valuation argument claims that the failure indications that people are not very concerned about their privacy. 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 then 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 merely 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 mid-size to large organizations, these contracts can number in the hundreds or thousands. The extent to 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 preventing designs that could lead to consumer harm or establishing processes for designers to use to better evaluate the risks new technologies pose.

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

The purpose of this Article isn't 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 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.

The conclusions that many commentators draw after invoking the privacy paradox – that people's behavior demonstrates that people really don't value privacy and that privacy protection thus isn't necessary – are

completely wrong.

The privacy paradox is best interpreted not as an indication of how much people value privacy. Instead, the phenomenon demonstrates behavior involving risk, where many factors might influence people's decisions.

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 paradox because of conflated issues and flawed logic.