Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms

Kirsten Martin
George Washington University

ABSTRACT: The oft-cited privacy paradox is the perceived disconnect between individuals' stated privacy expectations, as captured in surveys, and consumer market behavior in going online: individuals purport to value privacy yet still disclose information to firms. The goal of this paper is to empirically examine the conceptualization of privacy postdisclosure assumed in the privacy paradox. Contrary to the privacy paradox, the results here suggest consumers retain strong privacy expectations even after disclosing information. Privacy violations are valued akin to security violations in creating distrust in firms and in consumer (un)willingness to engage with firms. This paper broadens the scope of corporate responsibility to suggest firms have a positive obligation to identify reasonable expectations of privacy of consumers. In addition, research perpetuating the privacy paradox, through the mistaken framing of disclosure as proof of anti-privacy behavior, gives license to firms to act contrary to the interests of consumers.

KEY WORDS: consumer trust, privacy paradox, valuation of privacy, behavioral targeted advertising, corporate responsibility, duty

Current online marketing techniques utilize a robust picture of the consumer, and an information ecosystem comprised of data aggregators, data brokers, trackers, websites, and ad networks collects and stores online consumer information to facilitate targeted marketing. Yet, tactics integral to online marketing, such as consumer tracking and data aggregation, are found to be consumer concerns by popular and academic surveys (Leon et al. 2015; Martin 2015; Martin and Shilton 2016; Turow, King, Hoofnagle, Bleakley, and Hennessy 2009; Ur, Leon, Cranor, Shay, and Wang 2012).[1]

This tension—between consumers' stated privacy preferences, as measured in surveys, and their actual behavior, as measured by consumers' continued online activity—is referred to as the privacy paradox by academics and practitioners. Research on the privacy paradox explains that consumers may judge privacy as important in surveys but (paradoxically) continue to engage with websites and disclose information (Kokolakis 2017; Norberg, Horne, and Horne 2007; Strahilevitz and Kugler 2016). As noted by

[1] As noted by marketing professor Catherine Tucker, "The unusual feature of online advertising markets is that they are characterized by a tension between the desire of a firm to be informative to the right set of consumers, and consumers' apparent distaste for how firms use data" (Tucker 2012).

DOI: 10.1017/beq.2019.24

Kokolakis, continued proof of the privacy paradox in research encourages firms to increase the collection and use of personal information (2017). Consumer-facing firms, marketers, and advertising advocacy groups use the privacy paradox to justify their current data practices, while also reporting data that shows that consumers overwhelmingly find such practices problematic and creepy (Guest Author 2018; Lacy 2018).[2]

The privacy paradox is important for business ethics because the narrative of the privacy paradox defines the scope of corporate responsibility as quite narrow: firms have little to no responsibility to identify or respect privacy expectations, if consumers are framed as relinquishing privacy while online. While researchers continue to identify and explain conditions for the privacy paradox, a growing number of privacy scholars suggest that consumer behavior is not a reliable indicator of their privacy interests. In fact, the term 'paradox' is defined as "seemingly absurd or self-contradicting statement or proposition that, *when investigated or explained*, may prove to be well founded or true."[3] Framed in this manner, the oft-cited privacy paradox requires additional empirical testing, since current market behavior may not capture consumers' approval of the fact that a firm conforms to ethical norms.

The privacy paradox persists in the face of critiques because the concept relies upon a particular theoretical conception of privacy and type of privacy right. Where others have demonstrated problems with both surveys to measure privacy expectations, as well as problems with consumers' market decisions, here I examine the theoretical conceptualization of privacy and the type of privacy right assumed in the privacy paradox. The goal of this paper is to test the privacy paradox by empirically examining privacy expectations postdisclosure and measuring consumer valuation of privacy violations. As I explain, for the privacy paradox to persist, one of two assumptions is necessary: (a) that when consumers disclose information and engage with firms, they also relinquish privacy expectations, or (b) that privacy is a preference that is easily negotiated away in the market. Philosophers and legal scholars, on the other hand, argue that reasonable privacy expectations exist postdisclosure and that privacy is a right similar to a core value to be respected at all times. Through a series of four factorial vignette surveys, the importance of consumer privacy norms is compared to both the benefits of sharing information and clear violations, such as security breaches. A trust game experiment then quantifies the impact that violating privacy norms has on consumers' willingness to engage with a market actor. In doing so, this study measures the scope and valuation of privacy using both a survey technique designed to combat respondent bias, as well as actual behavior in an experiment when market actors are fully informed and given a choice.

If, as shown here, disclosure is not a meaningful point at which privacy is compromised, then (1) consumers are not acting paradoxically when going online,

[2] As reported by marketing and advertising firms, a report by Gartner asked respondents how consumers felt about "online ads that use details about what I have done" and found that 73 percent of consumer responses were negative (49 percent used a version of creepy), whereas respondents who were marketers insisted that consumers found the same practice "valuable" when engaging online (Dodd 2016), as well as specific firms such as Facebook—"How Facebook uses the privacy paradox to keep users sharing" (Glance 2018).

[3] *Merriam-Webster Dictionary,* online, s.v. "paradox," italics added. https://www.merriam-webster.com/dictionary/paradox. I thank Alessandro Acquisti for pointing out the actual definition of paradox in reference to the privacy paradox.

and (2) firms have a very different type of obligation to understand and respect the privacy of consumers. Where firms currently are framed as having, at most, a duty to not interfere with consumers choosing to relinquish privacy, this paper broadens the scope of corporate responsibility to suggest firms may have a positive obligation to identify reasonable expectations of privacy of individuals. Finally, the results impact how privacy is conceptualized and empirically examined in business ethics; research perpetuating the privacy paradox through the mistaken framing of disclosure as proof of anti-privacy behavior is harmful as it gives license to firms to act contrary to the interests of consumers.

PRIVACY PARADOX

The privacy paradox, as a concept, attempts to reconcile consumer behavior with privacy concerns as measured in surveys.[4] Despite critiques of the operationalization of the privacy paradox in empirical work, the privacy paradox persists as an explanation for consumer behavior in research, with implications for the role of firms in respecting privacy (Chamorro-Premuzic and Nahai 2017; Kokolakis 2017). Research seeking to validate the privacy paradox first captures a general privacy concern or expectation in a survey and then compares the stated preference with self-reported disclosure of information or actual disclosure to a researcher (Dienlin and Trepte 2015). Importantly, the researchers equate the disclosure of information to "privacy compromising behavior" (Barth and de Jong 2017) in validating the privacy paradox. Alternatively, researchers questioning the privacy paradox demonstrate problems with both surveys to measure privacy expectations, as well as problems with consumers' market decisions as revealing preferences. Scholarship supporting and undermining the privacy paradox is summarized in Table 1.[5]

However, for the privacy paradox to persist as a valid concept to consider, consumers must be able to act 'paradoxically' in regards to privacy expectations online. In other words, the paradox is important to examine and theorize about, if, and only if, consumers are possibly acting in an anti-privacy manner when sharing the information. Framing the handoff of information as dispositive of relinquishing privacy is critical to the possibility of the privacy paradox—otherwise there is no paradox or incongruent behavior to explain.

For disclosing information to firms or just going online to be considered privacy-compromising behavior, we must assume either that (1) individuals relinquish privacy when online and have no expectations of privacy (a strong privacy paradox) or

[4] Most scholars reference work from mid-2000s as that is when scholars began using the privacy paradox (Barnes 2006; Norberg, Horne, and Horne 2007). Etzioni used the phrase earlier in 1999, but in reference to the paradox that privacy-minded individuals would have to rely on Big Brother (government), whom they normally loathe, in order to keep Big Bucks (firms) in check in regards to protecting privacy (Etzioni 1999).

[5] First, measurements of privacy concerns and privacy expectations are seen as grossly simplified, and consumers have nuanced expectations about who has access to and use of their data—even data deemed sensitive (Martin and Nissenbaum 2017a). Second, actual online behavior may be a poor proxy for consumer privacy expectations.

Table 1: Examples of Research on the Privacy Paradox

	Scholarship *Validating* the Privacy Paradox	Scholarship *Undercutting* the Privacy Paradox
Surveys as Adequately Measuring Privacy Preferences	Privacy concerns do not predict social network use, since respondents' stated privacy concerns in a survey, but still reported use of social networks when asked (Baruh, Secinti, and Cemalcilar 2017).	Surveys with broad questions about privacy concerns or valuations of privacy do not capture individuals' privacy judgements about specific sharing and use of information (Martin and Nissenbaum 2017a). When respondents are asked specifically about the secondary use of consumer data, their responses do predict privacy-protecting behavior (D'Souza and Phelps 2009).
Disclosure as a Proxy for Privacy Expectations Being Met	Consumers do not uphold their stated concerns when going online (Kokolakis 2017; Norberg, Horne, and Horne 2007; Strahilevitz and Kugler 2016; Young and Quan-Haase 2013).	Cognitive biases explain how consumers make myopic or narrow decisions when they discount privacy harms (Acquisti, Brandimarte, and Loewenstein 2015).
	Scholars examine the mechanisms, such as theory of planned behavior (TPB) (Dienlin and Trepte 2015) and communication privacy management (CPM) (Baruh, Secinti, and Cemalcilar 2017), to explain consumers' paradoxical behavior.	Consumers employ nuanced protection schemes when online (Hargittai 2010; Tufekci 2008; Young and Quan-Haase 2013). Information asymmetries impede consumers' ability to make informed decisions while online (Acquisti, Brandimarte, and Loewenstein 2015). Consumers have difficulty identifying the actual practices of firms (Englehardt and Narayanan 2016). Consumers project their privacy expectations onto ambiguous privacy notices, suggesting consumers believe privacy is respected when engaging online (Martin 2015).

(2) individuals 'trade' privacy interests in return for something (a weak privacy paradox). I explain the strong and weak versions of the privacy paradox and associated hypotheses below. I also explain that how we frame and acknowledge the importance of respecting privacy expectations has implications for not only the role of firms in respecting privacy, but also the type of duty firms have to respect privacy.

The No-Privacy-Exists Argument (Strong Privacy Paradox)

The strongest version of the privacy paradox, whereby consumers have no privacy expectations online regardless of their claims in surveys, assumes that disclosing information by visiting a website or using an application connotes *relinquishing* privacy expectations. This approach is exemplified when disclosure is considered "privacy compromising behavior" (Barth and de Jong 2017), or anti-privacy behavior (Baruh, Secinti, and Cemalcilar 2017). Being visible, or making information accessible, flips a switch where, as Nissenbaum nicely summarizes, we (mistakenly) argue 'anything goes' (2010).

This strong version of the privacy paradox relies upon a particular definition of privacy. While scholars agree that privacy, in general, is important to develop, as individuals, in order to have a sense of autonomy, foster relationships and intimacy, and support society (Allen 1988; Cohen 2012; Inness 1996; Nissenbaum 2010; Regan 1995), we do not agree on, what Schoeman calls, the substantive argument about privacy or what it means when we say 'privacy' (Schoeman 1984).

Two definitions of privacy support the view that disclosure, or going in public, connotates relinquishing privacy. Both privacy as that-which-is-inaccessible (Allen 1988; Parent 1983; Warren and Brandeis 1890) and privacy as that-which-is-controlled (Milne and Culnan 2004; Moore 2010; Ruedy et al. 2013; Sheehan and Hoy 2000; Westin 2003) support disclosure as the critical point where privacy is compromised. For privacy as that-which-is-inaccessible, individuals are in a private state when they are separated or inaccessible to others. Pure privacy is a state of isolation; walking in public and going online makes one accessible and, therefore, not private. For the control version of privacy, whereby an individual has privacy if they have control over themselves and their information, going online (or in public) relinquishes the degree of control one has over information about themselves and, therefore, constitutes privacy-compromising behavior. In both existing conceptualizations of privacy, disclosing information is equivalent to privacy-compromising behavior due to making information accessible or due to consumers relinquishing control (Gabisch and Milne 2014; Milne and Gordon 1993). When online, the use of information by third parties after disclosure—e.g., selling information to a data aggregator, using information to sell consumers insurance, storing information for later use—would not be a concern for consumers according to this strong version of the privacy paradox, as they are assumed to have relinquished privacy expectations when going online. This assumption concerns the very definition of what it means to respect privacy and constitutes the strongest form of the privacy paradox: consumers, who may claim to have privacy expectations and concerns in surveys, yet continue to transact with firms online, *are hypocritical*. No privacy expectations exist postdisclosure.

Argument #1: Individuals have no reasonable expectations of privacy after disclosing information. Therefore, engagement online means, by definition, that consumers relinquish their privacy expectations.

Within the strong version of the privacy paradox, firms have no responsibility to understand let alone meet consumer privacy expectations any more than firms could decide to understand and meet consumer preferences as to what bottled water is offered to employees or the color of the paint on their walls. If consumers have no legitimate privacy interests once information is disclosed to a firm, then firms are given license to share, aggregate, and use the information they collect. Any actions of the website—to whom the consumer disclosed information—would be within the norms of the consumer-firm relationship, and selling information to third parties for any use would be expected.

Importantly, actions that conform to the norms of the relationship and expectations of the firm build trust, and actions that violate norms and unmet expectations

detract from trust, since these norms form the guidelines of appropriate behavior within the relationship (Cropanzano and Mitchell 2005). If the consumer-facing firm behaves within the norms and expectations of the relationship—and meets their obligations—then we would expect either a positive impact on trust or, at least, a non-negative impact on trust. Privacy expectations are no different; privacy expectations are critical to a relational exchange online, where norms and trust are central and consumers are vulnerable (Vargo and Lusch 2004; Sirdeshmukh, Singh, and Sabol 2002). Therefore, individuals will judge sharing with third parties and using data outside the immediate context to be within the expectations of the relationship: the consumer-facing firms would have met their obligations and the actions would *not* be a breach of trust.

H1a: The use of consumers' online information postdisclosure by third-party marketers will not negatively impact consumer trust in the website.

Alternatively, context-dependent approaches to privacy, such as privacy as contextual integrity (Nissenbaum 2010) and privacy as a social contract (Martin 2016), suggest individuals have expectations about the type of information that is accessed by an actor and subsequently used and shared with a given community; whether an information flow is appropriate or not depends on the agreed upon norms of the community. Privacy violations, therefore, are the breaches of these norms—when the type of information is given to the wrong person or used in an inappropriate way (Martin 2016). For example, health information shared with an insurance company is expected to be used to determine prescription coverage, but not to be later used by a bank to determine financial stability.

Importantly, context-dependent approaches place no special focus on mere disclosure as suggestive of less privacy. Individuals retain reasonable expectations of privacy at work, in public, when online, when at school, when attending a rally (Martin and Nissenbaum 2017b; Nissenbaum 1998). The appropriate norms of information flow would apply regardless of who has access or where the information is shared. For example, information shared with a retailer falls under a set of rules about who can receive that information and how it can be used: selling shopping information to a university for admissions decisions would be inappropriate and a privacy violation. Similarly, using voting records for an employment or education decision is considered inappropriate and a privacy violation—even if the voting information is available via public records (Martin and Nissenbaum 2017b). How websites gather, store, share, and then use information online is subject to privacy norms; consumers have privacy concerns and perceive there to be violations of privacy when information is shared, stored, or used in a manner deemed inappropriate for that particular context.

Previous work has identified secondary uses of information by third parties as a privacy concern among consumers (Belanger et al. 2002b; Flavián and Guinalíu 2006; Martin, Borah, and Palmatier 2016; Stewart 2016), including specific third party use of information for data brokers and marketing (Martin 2014; Madden 2014; Rainie et al. 2013; Turow, Hennessy, and Draper 2015). Therefore, where the dominant approach to online privacy norms relies upon consumers relinquishing privacy expectations upon disclosure, privacy as context-dependent norms suggests

that consumers will judge sharing data with third parties and using it outside the immediate context to be a violation of the privacy norms of the consumer exchange relationship and a breach of trust.

H1b: Alternatively (and undercutting Argument #1), the use of online information post-disclosure by third parties negatively impacts consumer trust in the website.

The Privacy-Can-Be-Traded Argument (Weak Privacy Paradox)

A weaker version of the privacy paradox suggests that consumers may retain reasonable privacy expectations after disclosure, yet demonstrate their willingness to 'trade' the risk of a privacy violation for the many benefits of sharing information online. According to this view, consumers regularly exchange their privacy preferences for the benefits of discounts, better service, or social affiliation (Hui, Teo, and Lee 2007; Schumann, von Wangenheim, and Groene 2014; Xu, Zhang, et al. 2009). This exchange approach to privacy frames consumers as taking into consideration the risks and benefits of disclosing information when assessing privacy concerns and expectations (Culnan and Bies 2003; Dinev and Hart 2006; Hui, Teo, and Lee 2007; Xu, Teo, et al. 2009). And the justifications for relinquishing privacy interests are diverse: consumers are willing to disclose information for personalization (Xu, Teo, et al. 2009), as well as free services and useful ads (Banerjee and Dholakia 2008).

While consumers may express concerns about marketing online or even find pervasive tracking as a violation of the privacy norms, as hypothesized in H1b, a weaker privacy paradox suggests that privacy norms may be important, but need to be put into the perspective of the possible benefits of being online. Uses of information deemed privacy violations in consumer surveys may be better judged after taking into consideration the benefits of sharing information online. According to the weaker privacy paradox, consumers retain privacy interests after disclosing information, but those interests are easily traded in the market (Barth and de Jong 2017). Privacy is closer to a preference; consumers are regularly unconcerned about respecting privacy interests online and trade privacy within their market utility function. Consumers are considered unconcerned or pragmatic in their willingness to exchange privacy for benefits (Westin 2001).

With the weaker version of the privacy paradox, firms' obligations in regards to privacy center on a duty to not interfere with the rights of consumers to choose as market actors. In considering duties for firms or individuals, obligations can be positive where an individual has an affirmative duty to protect the rights of others. For a firm, this could include a positive duty to ensure employees are not harmed. However, negative duties are when a firm has a lower obligation to not get in the way of an individual exercising their rights (Shue 1996). A negative duty could include not deceiving employees in regards to pay. Here, firms would have a negative obligation to not interfere with consumers seeking to bargain in the market.

According to the weak version of the privacy paradox, privacy is assumed to be valued as a utility function in the market, with firms having an obligation to not interfere within the market for privacy preferences. Firms may have a negative duty to not hinder consumers' ability to trade away their privacy preferences and choose

corresponding market transactions. Firms can do with the information what they want as long as the information was not gathered with deception or fraud. When consumers go online, their privacy concerns are assumed to be overwhelmed by the benefits of targeted advertising and using a particular website (e.g., the quality of the news, the pleasure of watching videos, etc.).

This assumption concerns the value consumers place on privacy and constitutes the weaker form of the privacy paradox: consumers, who may claim to have privacy expectations and concerns in surveys, yet continue to transact with firms online, are easily bought.

Argument #2: Privacy is a preference; individuals exchange privacy for benefits online; violations are worth the many benefits of sharing information.

H2: Consumers perceive the benefits of sharing information to outweigh any perceived harms and risks from privacy violations through the secondary use of information.

Privacy-As-Core-Value Argument (No Paradox)

Alternatively, and undercutting the idea of a privacy paradox, consumers may be consistent in stating privacy concerns and expectations in surveys, while also retaining those concerns and expectations after engaging with a website. In going online, consumers expect firms to respect the privacy norms as to who has access to what information and how that information is used. Scholars who make normative claims about privacy have been arguing for privacy as a core value, which is necessary for individual autonomy and development, to foster intimacy and relationships, and for societies to flourish (Cohen 2012; Nissenbaum 2010; Regan 1995). Core values are not considered negotiable and are positive goals we seek to attain and require in our communities (Donaldson 2003; Donaldson and Walsh 2015).

Importantly for business ethics, if consumers have a privacy right akin to a core value, then firms would have a positive obligation to identify and respect the privacy expectations of consumers around the information they gather, or allow to be gathered, due to their relationship with the consumer (Arnold 2010; Donaldson and Dunfee 1994; Shue 1996).

One core value where firms have a positive duty to protect consumers is in the area of security. In general, security is part of the United Nations Declaration of Human Rights, in that individuals have a right to protection from arbitrary interference with one's communications. More recently, the UN Commission on Human Rights focused on the protection of individuals from intrusions in a digital life. Consumer concerns about the security of their data has only solidified in recent years after well-known cyber attacks on specific firms, such as Target, the *New York Times*, and even the Office of Personnel Management (OPM). Firms' consumer information security practices are increasingly the subject of government scrutiny through the Federal Trade Commission (FTC), as well as through regulations of specific industries, such as with the Financial Industry Regulatory Authority (FINRA) or the Health Insurance Portability and Accountability Act (HIPPA). The Securities and Exchanges Commission (SEC) has elevated the issue of cybersecurity to the

level of the board of directors of public companies to help maintain the integrity of these markets (Aguilar 2014).

Just as beneficial uses of information help put into perspective the importance to consumers of privacy norms in H2 above, comparing the importance of violating privacy norms to clear violations of an important value—such as a security violation—can place a lower bond on the relative valuation of privacy norms. Where privacy violations are actions firms take that treat information inappropriately, security violations are outsiders (e.g., hackers or governments) who cause harm by damaging a system or accessing, disclosing, and misusing consumer data (Belanger, Hiller, and Smith 2002; Flavián and Guinalíu 2006; Miyazaki and Fernandez 2000).

While surveys have shown a relationship between consumer concerns about security and privacy (Pew Research Center 2014), the risks to the consumer as evidenced by regulators' attention and standards of practice should be substantially greater for security violations as compared to privacy norm violations.[6] Therefore, security violations would constitute a lower bound on violations of the norms of the consumer-firm relationship as we would expect; when directly asked, consumers judge security violations to be well outside the norms of the relationship.

Argument #3: Privacy is a core value to be respected.

H3. Privacy violations will have a negative impact on consumer trust in the website similar to violations of established core values, such as security.

OVERVIEW OF STUDIES

The goal of this paper is to test the privacy paradox and empirically examine the theoretical conception of privacy assumed in the privacy paradox. The hypotheses above examine the scope and relative importance of violating consumer privacy norms related to the use of disclosed information. To this end, a factorial vignette survey methodology was used to test the scope and relative importance of violating consumer privacy norms online. Factorial vignette survey methodology was designed to investigate human judgments using highly contextual vignettes (Jasso 2006; Rossi and Nock 1982). In a factorial vignette survey, a series of vignettes is generated for each respondent, comprised of a general framework, with specific vignette factors systematically varied within each scenario. The vignette factors, which are the independent variables for the study, are controlled by the researcher and randomly selected. Respondents are asked to evaluate each hypothetical situation with a single rating task (Jasso 2006).

The vignettes allow the respondent to see realistic scenarios and judge the degree of trust or distrust in the website. The methodology is designed to avoid respondent bias whereby respondents attempt to answer surveys in a manner that is socially desirable. By changing the factors randomly through replacement, respondents see a new combination of vignette factors each time. Later analysis allows the researcher

[6] Consumers may not realize how intertwined trackers and targeted ads are with security concerns: ad networks have been used to install ransomware on consumers' computers by hackers (Trimm 2016).

Table 2: Assumptions of the Privacy Paradox

	Assumption	Philosophical Definition of Privacy	Firm Obligation
Privacy Paradox Assumptions	1. Disclosure of information signals that the consumer has no privacy expectations.	Privacy is information that is inaccessible or controlled by an individual. Individuals give up privacy upon disclosure since information is then accessible or controlled by the firm.	Individuals are assumed to have no privacy interests about disclosed information. Firms have no obligations in regards to selling, aggregating, or using information disclosed by consumers.
	2. Disclosure of information is a signal that the consumer has bargained away privacy in exchange for better service or products or for a discount.	Privacy is a preference that is negotiated in the market in exchange for benefits.	Firms have a negative obligation to not get in the way of consumers seeking to bargain in the market. Firms can do with the information what they want, as long as the information was not gathered with deception or fraud.
	3. Privacy is a core value essential for individual autonomy and societal development.	Privacy, as social contract norms negotiated within a context or community, is deemed critical to develop as individuals attempt to nurture relationships.	Firms have a positive obligation to identify the privacy expectations of consumers and ensure minimum core privacy expectations are met.

to identify the relative importance of each factor and level in order to move the rating task. Importantly, the factorial vignette methodology enables researchers to simultaneously examine multiple factors—e.g., the benefits and possible harms of the use of information or privacy versus security violations as hypothesized above—using vignettes that are systematically varied (Ganong and Coleman 2006).

Factorial Vignette Survey Design

Respondents were assigned one of four surveys and prompted to rate the degree to which they trusted a series of forty hypothetical websites. Common to all survey vignettes was a general overview about the type of information tracked by the website to include respondent location, demographic, history of websites they visited, and information only voluntarily provided. In addition, the website's purpose—such as banking, photo sharing, search, travel—and the duration of time the information was stored varied randomly across the vignettes. This provided a realistic common backdrop for all four factorial vignette surveys according to context-dependent approaches to privacy. See Table 3 for vignette factors. Table 4 includes the sample vignettes across survey runs where the secondary use of information and security violation are added to a base vignette, which is about beneficial uses of information. The levels for each factor were dynamically assigned as the respondent was shown the vignette to rate.

Table 3: Factorial Vignette Factors

Factor	Levels	Operationalized
Primary Use	TailorUse	Tailor services for you
	DiscountUse	Offer you discounts
	ImproveUse	Provide a faster and more user-friendly website
	AdUse	Place advertising targeted to you
Secondary Use	Friend2ndUse	The site sends advertising to friends and contacts
	Sell2ndUse	The site sells to a tracking company who combines the data with your other activities
	Research2ndUse	The site may conduct research experiments using you and other users
	Internal2ndUse	The site removes your name from the data and uses the data to improve their service
	Null2ndUse	Null
Security	Hacker	An outsider then used a flaw in the website to download user records
	NiceHack	A researcher then found a flaw in the website to suggest a security fix
	Law	The information is stored and easily available to law enforcement as needed
	Null	Null

Respondent Controls in Each Survey

Before and after the vignettes, the respondents were asked several control questions. Respondents' age and gender were collected before the vignettes, whereas the privacy, online knowledge and experience, and trust controls were asked after the vignettes to avoid priming the respondents. See the table in Appendix A for the control variables included.

The respondents' disposition towards trust and privacy were captured as a respondent-level control. The respondents' degree of institutional trust in the environment has been captured by a single rating task as a control previously in the trust literature, in order to differentiate trust in the institution from a user's trust in a specific firm or website (Pirson, Martin, and Parmar 2017; Pavlou and Gefen 2004). Individuals vary in their general trust disposition and their trust in an institution, such as business, online, or congress. Similarly, individuals' general concern about privacy, or belief that privacy is important, explains a portion of any individual judgment that privacy has been violated. In the privacy literature, experiments use single item controls to lower the demands on the respondents (Grossklags and Acquisti 2007). Respondent knowledge and technical experience have been important in other surveys of online trust (Leon et al. 2015) and were captured here (Martin 2018).

Rating Task

Consistent with the factorial vignette survey methodology, a single rating task remained the same for all vignettes (Jasso 2006; Wallander 2009). The single rating task assigned to a vignette is a strength of the methodology and is considered best practice (Jasso 2006; Auspurg et al. 2014; Rossi and Nock 1982). The single rating

Table 4: Vignettes Tested in Each Survey

	Survey Templates and Examples			
	Survey 1*	**Survey 2**	**Survey 3**	**Survey 4**
	Primary Use	Primary Use + Secondary Use	Primary Use + Security	Primary Use + Secondary Use + Security
Template				
	A {Context} silently collects {Information}.	A {Context} silently collects {Information}.	A {Context} silently collects {Information}.	A {Context} silently collects {Information}.
	The {Context2} site uses the data to {Use} and stores the data for {Storage}.	The {Context2} site uses the data to {Use} and stores the data for {Storage}.	The {Context2} site uses the data to {Use} and stores the data for {Storage}.	The {Context2} site uses the data to {Use} and stores the data for {Storage}.
		{SecondUse}	{Security}	{SecondUse}
				{Security}
Example				
	A travel website silently collects the history of websites you visited.	A general online search site silently collects your gender and age.	A travel website silently collects the history of websites you visited.	A general online search site silently collects the history of websites you visited.
	The travel site uses the data to provide a faster and more user-friendly website and stores the data for 10 years.	The search site uses the data to offer you discounts and stores the data for 10 years.	The travel site uses the data to provide a faster and more user-friendly website and stores the data for 10 years.	The search site uses the data to tailor services for you and stores the data for 10 years.
		The site keeps the data to possibly conduct research experiments using you and other users	An outsider then used a flaw in the website to download user records	The site keeps the data to possibly conduct research experiments using you and other users.
				An outsider then used a flaw in the website to download user records.

* Survey 1 tests if primary uses of information positively impact trust and serves as a baseline trust measurement for later comparison. The results illustrate that the use of information to tailor services ($\beta = +8.48$, $p < 0.005$), offer discounts (+6.33), and improve the website (+14.03) positively impacts trust, thereby supporting that consumers disclose information with an understanding of the beneficial, primary use of that information.

task—similar to a behavioral experiment with a single act—forces the respondent to make tradeoffs of theoretically important factors. In this case, the respondent is forced to make tradeoffs between contextual factors, such as (a) the beneficial use of information, (b) the secondary use of information, and (c) a security violation.

The focus of Surveys 1–4 is the highly particular consumer trust in a firm. Importantly, actions that conform to privacy norms build trust, and actions that violate privacy norms detract from trust, since these norms form the guidelines of appropriate behavior (Cropanzano and Mitchell 2005). Without trust, consumers are likely to disengage from the primary website that is tracking their behavior: the formation of trust is key for a consumer's "willingness to engage in an exchange relationship" at the level of vulnerability required online (Johnson and Selnes 2004, 4). This willingness to engage is the outcome of the experiment described below. For each vignette, respondents were instructed: "Tell us how much you agree with the statement below. Using a sliding scale from 'strongly disagree' to 'strongly agree.' Respondents rated their agreement with the following prompt for each vignette: "I trust this website."[7]

Sample

The surveys were deployed one at a time over the course of three months through Amazon's Mechanical Turk (MTurk), a crowdsourcing marketplace where researchers publish a job (a 'human intelligence task,' or HIT) for respondents to take a survey. Each respondent rated forty vignettes, taking approximately 10–12 minutes, as described in Table 4 and summarized in Table 5. US respondents were paid $1.70 and were screened for over 95 percent HIT approval rate. The survey implementation was designed to assuage a number of identified concerns with samples from MTurk. See Appendix B (available as an online supplement) for a detailed explanation of common concerns with MTurk, as well as how the study was designed to assuage those concerns—including gaming by respondents, demographic differences, and low motivation.

Analysis

The factorial vignette methodology creates a unique dataset with forty judgments or ratings for each respondent. The resulting data set can be thought of in two levels: the vignette contextual factors and the respondent control variables. Multilevel analysis was used to capture the degree to which variation in the rating task is attributable to the individual rather than the vignette factors (xtmixed in stata). In addition, each control variable was grouped with the scores broken into quartiles. Each control variable was captured using as slider with a scale of strongly disagree (-100) to strongly agree (+100). To create a relative score for each respondent, a new variable was created and assigned to each respondent as to what quartile their rating corresponded to (top 25 percent, bottom 25 percent, etc., of all ratings).

TESTING ARGUMENT #1: STRONG PRIVACY PARADOX

Argument #1 states that individuals have no reasonable expectations of privacy after disclosing information regardless of their stated concerns in surveys. H1a hypothesizes

[7] See also Rossiter (2002) on single item measures, as well as Schumann, von Wangenheim, and Groene (2014) on the tension in marketing literature around single item measures. The factorial vignette survey methodology relies on a single rating task by design as the multiple vignette factors capture the complexity of the concept.

Table 5: Descriptive Statistics of Surveys 1-4

	Survey 1		Survey 2		Survey 3		Survey 4	
	Primary Use		Primary + Privacy		Primary Use + Security		Primary + Privacy + Security	
Sample Statistics								
N (Users)	393		381		400		399	
N (Vignettes)	15,720		15,240		16,000		15,960	
DV Mean	-8.47		-16.98		-18.43		-25.23	
DV SD	28.95		29.46		28.25		27.35	
ICC Null	28.8%		27.1%		26.9%		25.0%	
Respondent R^2	0.695		0.744		0.711		0.742	
Respondent Control Variables	**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**
Knowledge Internet	2.90	0.97	2.74	0.95	2.86	0.96	2.85	0.93
Privacy Concern	55.46	40.15	58.21	42.53	59.31	36.98	61.53	38.11
Trust in Websites	-11.77	48.40	-13.49	48.89	-8.86	49.22	-13.83	48.94
Coding Experience	2.07	1.21	2.05	1.15	1.99	1.16	2.10	1.20
Privacy Important	78.51	26.47	81.90	24.25	80.07	25.16	82.51	23.07
Gender	1.41	0.49	1.45	0.50	1.45	0.50	1.39	0.49
Age	3.28	1.08	3.31	1.00	3.33	1.11	3.30	1.08

Note. DV = dependent variable. SD = standard deviation. Control variables are defined in Appendix A.

that the use of consumers' online information postdisclosure by third-party marketers will not negatively impact consumer trust in the website.

To test how secondary use of information postdisclosure by third-party marketers will impact consumer trust in the website, two surveys were run that included two types of uses postdisclosure: the primary (beneficial) uses of information (Survey 1 and 2) and the secondary use of information by marketers (Survey 2). The secondary use of information for marketing was operationalized as selling to a data aggregator, sending advertising to friends and contacts, conducting research, and improving the website's service in order to include both alternative uses of information, as well as alternative actors. Figure 1 illustrates the vignette factors by use and actor.

The scenarios presented in the vignettes looked like the following for Survey 2, where the bolded statement was appended to Survey 1 (bold text indicates new to this survey, but text was not bolded in the actual survey). The underlined portion changed based on the levels in Table 3.

> **Template:** A general online search site silently collects the history of websites you visited. The search site uses the data [Primary Use] and stores the data [Duration]. **[Marketing Secondary Use]**.
>
> **Example**: A general online search site silently collects the history of websites you visited.

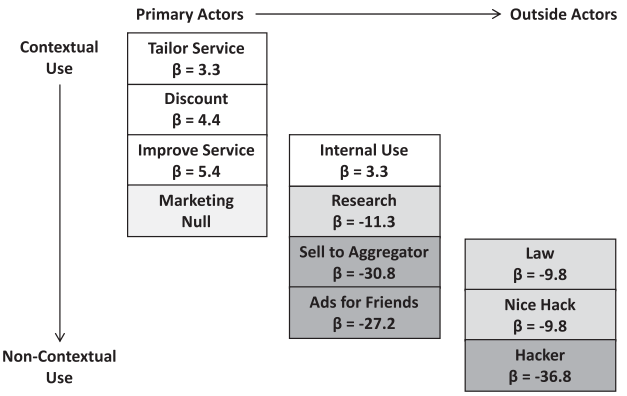

Figure 1: Vignette Factors By Contextual Use and Primary Actor

Note. Coefficients shown are from Table 6. Shading signifies negative impact on consumer trust; absence of shading signifies positive impact on consumer trust.

> The search site uses the data to tailor services for you and stores the data for 1 year. **The site keeps the data to possibly conduct research experiments using you and other users**.

The Trust Judgment equation was as follows:

(1) Trust Judgment = $Y_{ij} = \beta_0 + \beta_n \underline{\text{PrimaryUse}} + \beta_m \underline{\text{Marketing2ndUse}} + \Sigma\gamma_h R_{hi} + u_i + e_j$

Where,

- $\underline{\text{Primary Use}} = \beta_1 \text{TailorUse} + \beta_2 \text{DiscountUse} + \beta_3 \text{ImproveUse}$
- $\underline{\text{Marketing 2}^{nd} \text{ Use}} = + \beta_{11} \text{Friend2ndUse} + \beta_{12} \text{Sell2ndUse} + \beta_{13} \text{Reserch2ndUse} + \beta_{14} \text{Internal2ndUse}$

The term β_i measures the effect of the consumer being exposed to the primary and secondary use of information in the vignette. For example, β_1 measures the importance of using the information to tailor services to the consumer rather than the null (using information to place an ad).

To examine if the secondary use of information postdisclosure was a violation of trust, the dependent variable—consumer trust in the website—was regressed on the vignette and respondent factors for Survey 2. The results are in Table 6. The results show that two secondary and non-contextual uses of information, selling information to a data aggregator ($\beta = -48.77$, $p < 0.005$) and using information to target contacts and friends ($\beta = -46.75$, $p < 0.005$), negatively impacts trust of the firm even when the scenario contains beneficial uses of information and general context of the use of information. These findings do not support a strong version of the privacy paradox: H1a, which stated the secondary use of consumers' online information by third-party marketers will not negatively impact consumer trust in the website, was not supported. Consumers retained strong privacy expectations as to the use of information online.

Instead, H1b—that the secondary use of online information by third-parties will be judged to violate consumer privacy and, therefore, negatively impact consumer

Table 6: Multilevel Regression Results for Survey Experiments

Multilevel Regression of Rating Task on Vignette Factors								
Vignette Factors:	**Survey 1**		**Survey 2**		**Survey 3**		**Survey 4**	
	Primary Use		**Primary + Second Use**		**Primary Use + Security**		**Primary + Second + Security**	
	β	**SE**	**β**	**SE**	**β**	**SE**	**β**	**SE**
Primary Use								
TailorUse	8.48**	0.88	7.14**	0.94	4.79**	0.92	3.31**	0.95
DiscountUse	10.63**	0.88	6.06**	0.93	5.87**	0.92	4.37**	0.94
ImproveUse	14.03**	0.88	7.80**	0.93	8.67**	0.91	5.48**	0.94
(null = Ad Use)								
Marketing Secondary Use								
Friend2ndUse			-46.75**	1.05			-27.22**	1.05
Sell2ndUse			-48.77**	1.06			-30.85**	1.05
Research2ndUse			-18.63**	1.04			-11.32**	1.05
Internal2ndUse			9.24**	1.05			7.00**	1.05
(null = No 2ndUse)								
Security Violation								
Hacker					-47.88**	0.92	-36.83**	0.94
NiceHack					-18.05**	0.92	-9.75**	0.94
Law					-16.29**	0.92	-9.78**	0.95
(null = No Hack)								
Statistics								
DV (Ave Vignette Rating)	-8.47		-16.98		-18.43		-25.23	
SD (Vignette Rating)	28.95		29.46		28.25		27.35	
ICC Null	28.8%		27.1%		26.9%		25.0%	
Respondent R^2	0.695		0.744		0.711		0.742	
N (Users)	393		381		400		399	
N (Vignettes)	15720		15240		16000		15960	

Note. DV = dependent variable; SD = standard deviation; SE = standard error; * $p < 0.01$; ** $p < 0.001$.

trust in the website—is supported. The results suggest that consumers consider the secondary use of information for marketing to be outside the acceptable privacy norms of the consumer-firm relationship; the results undercut the strong version of the privacy paradox where consumers may state privacy concerns in surveys but have no reasonable privacy expectations online.

TESTING ARGUMENT #2: WEAK PRIVACY PARADOX

Argument #2 states that privacy is a preference; individuals exchange privacy being respected for better services, ads, or discounts online; privacy violations are worth the many benefits of sharing information. Relatedly, H2 states that

regardless of the scope of privacy (H1a versus H1b), consumers perceive the benefits of tracking to outweigh any perceived harms and risks from privacy violations through the secondary use of information on consumer trust. To test H2, we examine the relative importance of the primary uses of information compared to the relative importance of the secondary uses of information. We would expect that the benefits of the primary use of information to outweigh, and even be significantly larger than, any potential costs associated with secondary uses on consumer trust.

The results show that the two secondary uses of information—sharing information with a third party (selling to a data aggregator) and changing the use of information (to target friends) —statistically have the same impact on consumer trust ($\chi^2 = 1.38$, $p = 0.24$), yet have significantly greater (negative) impact on trust in the firm than the primary uses of information. In fact, the addition of the secondary use of information to the vignettes drives down the average trust rating of the vignettes to -16.98 in Survey 2 compared to -8.47 for Survey 1, when only the primary use of information was included ($t = 13.53$, $p < 0.001$; cohen's $d = 0.153$ with 95 percent CI (0.131, 0.176)). The results support that the secondary use of information—to include selling to a data aggregator, using information to target friends, and conducting research on the consumer—negatively impacts consumer trust in a website and outweighs the positive impact of the primary use of information. The findings do not support H2 and the weak version of the privacy paradox: respondents did not perceive the benefits of tracking to outweigh the perceived harms and risks.[8] These findings suggest consumers do not 'trade' privacy for benefits.

TESTING ARGUMENT #3: PRIVACY AS A CORE VALUE

Surveys 1 and 2 examine the scope of privacy and whether privacy is a preference exchanged for benefits online. The results show that the negative impact on trust, as a result of the secondary use of information for marketing, outweighs the beneficial uses of information for the consumer. Both the strong and weak version of the privacy paradox were not supported, suggesting that consumers care how information is used postdisclosure more than is currently recognized. Yet, how far marketing practices are outside the privacy norms of the consumer-firm relationship is not clear. Argument #3 states that privacy is a core value to be respected. Further, H3 hypothesizes that privacy violations will have a

[8] In fact, the average trust rating for respondents was -8.47 when only beneficial primary uses were included, as shown in Table 4, suggesting that, on average, respondents distrust websites even for their primary use of information. However, the average trust rating for websites in the vignettes is more than the average institutional trust in websites, suggesting respondents trust specific websites more when the details of the primary use of information is described (institutional trust-in-websites = -11.77); in addition, the average trust rating when the data in the vignette is stored for only the immediate session is positive (+20.87). The results support an inference that the primary use of information positively impacts trust in the website, and that the average consumer trust in a website is positive when storage of information is minimized.

negative impact on consumer trust in the website similar to violations of established core values, such as security.

To further clarify if privacy is treated like a core value, Surveys 3 and 4 compare the impact of privacy violations and security violations on consumer trust. Security violations are outsiders (e.g., hackers) who cause harm by damaging a system or accessing, disclosing, and misusing consumer data (Belanger, Hiller, and Smith 2002; Flavián and Guinalíu 2006; Miyazaki and Fernandez 2000).

To test H3 and whether privacy violations are judged similar to security violations in impacting consumer trust, Survey 3 included the baseline vignette factors (Survey 1) plus security violations defined as an outside intruder accessing the websites' information about the consumer. To isolate the importance of an outsider with different intentions to do harm, three security violations were varied: a researcher identifying as security flaw to help the website (NiceHack), an outsider then using a flaw in the website to download user records (Hacker), and law enforcement having access to the data (Law). All are outsiders to the firm-consumer relationship with different intentions for the breach—see also Figure 1.

The scenarios presented in the vignettes looked like the following—bolded is new to this survey with the underlined portion varying based on the levels in Table 4.

> ***Template:*** *A general online search site silently collects the history of websites you visited. The search site uses the data [Primary Use] and stores the data [Duration].* ***[Security Violation]****.*
>
> ***Example:*** *A general online search site silently collects the history of websites you visited.*
> *The search site uses the data to tailor services for you and stores the data for 1 year.*
> ***A researcher then found a flaw in the website to suggest a security fix****.*

In Survey 3, Equation (1) is appended to include:

$$\text{Possible Security Violations}: + \beta_{15}\text{Hacker} + \beta_{16}\text{NiceHack} + \beta_{17}\text{Law}$$

H3 states that regardless of the scope of privacy (H1a versus H1b), privacy violations will have a negative impact on consumer trust in the website similar to violations of established core values, such as security. To test H3, the dependent variable—consumer trust in the website—was regressed on the vignette and respondent factors for Survey 3. The results are in Table 6 and Figure 1. Not surprisingly, security violations, in the form of an outsider gaining access to consumer information, negatively impacted trust in the website and outweighed the positive impact of the primary use of information.

However, and in support of H3, the impact on an individual's trust in a firm with a hacker accessing the data, as in Survey 3 ($\beta = -47.88$, $p < 0.005$), is the same as when a website sells information to a data aggregator ($\beta = -46.75$; $\chi^2 = 0.04$, $p = .85$) or uses information to target friends ($\beta = -48.77$; $\chi^2 = 0.52$, $p = 0.47$), as in Survey 2. In other words, consumers appear to equate violating privacy norms, such as a website selling information to a data aggregator or using the information to retarget friends, with security violations, in terms of distrusting the website. The

relative importance of secondary uses of information to consumer trust (Survey 2) is statistically equal to the outsider taking the data (in Survey 3).

To further test this surprising finding, Survey 4 was run to have the respondents directly compare the secondary use of information and security violations in the same vignette. The vignettes of Survey 4 included Survey 2 as a base (primary and secondary use of information), plus security factors. The results are in Table 6 and Figure 1. Here the negative impact of the security violations (β_{hacker} = -36.83, $p < 0.005$) has a slightly greater impact on consumer trust than secondary uses of information, such as selling information to a data aggregator (β_{sell} = -30.85, $p < 0.005$) or using to retargeting friends (β_{friend} = -27.22, $p < 0.005$), thus partially supporting H3.

When tested separately, a security violation of a hacker accessing consumer information diminishes trust in a website in a manner similar to violating privacy norms. However, when tested simultaneously in Survey 4, the impact of a security violation of an outsider gaining access to consumer information is slightly more negative than the violation of privacy norms.

TESTING PRIVACY AS A CORE VALUE, PART II: AN EXPERIMENT

In order to further test the finding that privacy violations are valued similar to a security violation by consumers, we sought to measure the impact of violating a privacy norm—the secondary use of consumer data for marketing—on the trust *behavior*, or a consumer's willingness to engage. A recurring limitation in capturing only the trust judgment of respondents is having no direct measure of their willingness to become vulnerable (McKnight, Choudhury, and Kacmar 2002).

One tool utilized in behavioral economics and organizational behavior research is the "trust game" to assess trust in a trustee (Anderhub, Engelmann, and Güth 2002; Berg, Dickhaut, and McCabe 1995). The trust game has been used to measure both trustworthy factors of partners, as well as general contextual factors that impact trusting behavior (Malhotra 2004; Malhotra and Murnighan 2002). In some surveys, the trust game (or investment game) is played between two people in a lab. Here, we are interested in an individual's trust in a website, so the respondent is assigned to be one player (Player 1) and plays the game online with a 'website' (Player 2) designed with particular attributes. Player 1 must decide to become vulnerable to Player 2 by passing the initial amount of money and trusting Player 2 will share the proceeds back.

Experiment Procedure

Participants were told they would play four rounds with the same partner, and each participant made four separate decisions. Each round of the scenario occurred in two stages as shown in Figure 2. For example, Player 1 was endowed with $0.30 at the start of each round. Player 1 then made the first decision and could pass $0.30 or take $0.30. If Player 1 chose "Take," they earned $0.30, Player 2 earned $0, and the round ended. If Player 1 chose "Pass" (Trust), the amount of money grew to $0.90, and Player 2 decided whether or not to share the $0.90 with Player 1 ($.45 for each). In each round, Player 1 indicated his or her choice. Participants

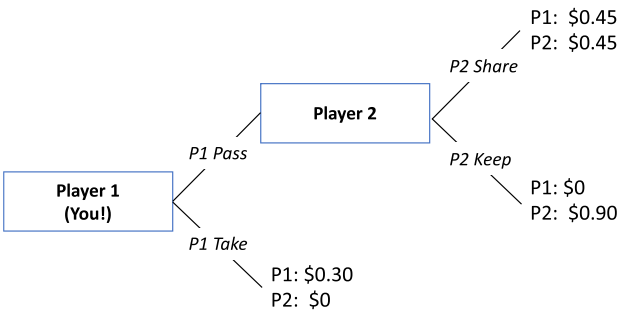

Figure 2: Diagram of Trust Game Experiment as Shown to Respondents

learned each round what Player 2 decided and could take Player 2's behavior into account in the next round.

The outcome was binary (0/1) as the respondent could only pass or not pass to Player 2. The experiment measures actual trust behavior rather than a normative judgment or trust intent. By changing the attributes of the programmed website, who is Player 2 (e.g., if Player 2 used privacy preserving ads versus pervasive tracking), we measured the trustworthiness of Player 2 as dependent on the contextual choices Player 2 made in regards to consumer racking.[9] After each of the four rounds, we also asked participants, "How much do you trust your partner?" (1 = completely trust, 7 = do not trust at all). Standard controls from the previous surveys were used.

The respondents received the following instructions:

> In this part of the experiment, you will make several decisions in an interactive scenario that allows two players to earn money—Player 1 and Player 2. You are Player 1.
>
> First, you will learn the rules of the scenario, and then you will learn the attributes of Player 2.
>
> The experiment consists of 4 rounds in total, and each player will make 4 separate decisions.
>
> Each round of the scenario occurs in two stages: In the first stage, you (Player 1) choose PASS (Invest) or NO PASS (Take).
>
> 1. If you choose NO PASS, the round ends and you earn $0.30.
> 2. If you choose PASS, then the money is tripled and Player 2 has $0.90 to either share or keep.
>
>   - If Player 2 chooses SHARE, then you both split the $0.90 and each earn $0.45.
>   - If Player 2 chooses KEEP, Player 2 keeps the $0.90 and you earn $0.00
>
> Bonus Payment: Within 24 hours after the experiment, we will choose one round from this scenario and you will receive a bonus payment based on your decision and the

[9] A meta-analysis of the trust game in economics found important differences in trusting an individual in a lab versus trusting an online source with a programmed agent, such as a website (Johnson and Mislin 2011). Since the actor of interest plays a role in a consumer's willingness to engage with a website, including Player 2 as a website most clearly replicated the actual phenomenon of interest.

decision of Player 2. This payment is in addition to your $1.00 payment for completing the HIT. You can also earn a bonus for paying attention throughout.

Thank you for participating!

After the control questions, respondents were told "You have been randomly assigned one of three possible versions of Player 2. For you, Player 2 is a website where the designer of the website wrote a program to respond to each of your decisions. *For full disclosure*: . . ." and then given one of three conditions:

A. *Privacy Preserving* (N = 227): In the course of his other work, Player 2 supports his website by offering ads without tracking the user specifically. The designer (Player 2) has decided to not disclose any personal information such as a user identifier or behavior to data brokers or ad networks.

B. *Ad Network* (N = 202): In the course of his other work, Player 2 supports his website by selling access to his users' behavioral information using an online advertising network that collects user behavior (browsing, purchases, searches, etc.) to offer highly personalized ads based on consumers' online history. Data brokers can then combine the consumer information from other sources online and offline for later use.

C. *Security Violation* (N = 227): In the course of his other work, Player 2 was unfortunately recently hacked and had user data downloaded by a third party. It is not clear who attacked the website.

Sample

American participants (N = 856) were recruited from MTurk (46 percent female and median age range of 25–34 years old). All respondents had a HIT approval rate of over 95 percent. Each participant received $1.00 for taking the survey regardless of the outcome of the experimental game. In addition, respondents would receive a bonus of up to $0.50 based on the results of the trust game and their overall diligence in taking the survey.

Results

To test if privacy violations are valued enough to negatively impact consumers' market behavior, the percent of respondents who passed to Player 2 (trusted Player 2, or at least were willing to engage with Player 2) was calculated for each round and by each type of Player 2 (Privacy Preserving, Ad Network, Security Violation). The results are in Table 7.

Table 7: Percent of Respondents Who Pass the Endowed Amount to Player 2 Each Round by Condition

		Percent Who Pass			
	N	**R1**	**R2**	**R3**	**R4**
Generic *	200	72%	73%	82%	76%
PrivacyPreserving	227	73%	78%	82%	81%
AdNetwork	202	64%	74%	73%	78%
Security Violation	227	64%	70%	77%	78%

* A separate survey was run without any mention of the privacy or security practices of Player 2. The results of the 'generic' Player 2 serve as a baseline here.

Table 8: Respondent Institutional Trust in Websites

	Trust Sites	Frequency	Percent	Cumulative
Low Trust	Not at All	24	3.66	3.66
	Slightly	159	24.24	27.90
Moderate Trust	Somewhat	306	46.65	74.54
High Trust	Moderately	162	24.70	99.24
	Completely	5	0.76	100
	Total	656	100	

Note. Table entries reflect responses to "In general, I trust websites online."

Partners who were described as using privacy preserving practices were trusted more frequently (73%) than partners who utilized privacy violating practices, such as pervasive tracking techniques (64%) (t = -1.96, p = 0.02; Cohen's d = -.19, 95% CI (-.38, 0.00)). In order to examine how respondents with high and low institutional trust differ in the trust game experiment, high trust was defined as a respondent who answered that they moderately or completely trust websites (a 4 or 5 in the control), and low trust was defined as respondent who stated they only slightly or not at all trusted websites, generally. This control question was asked before the experiment began. See Table 8.

Figure 3 shows no difference in initial trust or a willingness to engage between Player 2's conditions (privacy preserving versus ad network) for high-trusting respondents (25 percent of the sample). Perhaps most concerning for firms, moderate-trusting respondents (47 percent of the sample) were the most impacted by Player 2's decision to use an ad network and violate the privacy norms. Figure 3 shows 60 percent of moderate-trusting respondents were willing to engage with Player 2 using an ad network versus 75 percent who were willing to engage in round 1 for privacy preserving Player 2.

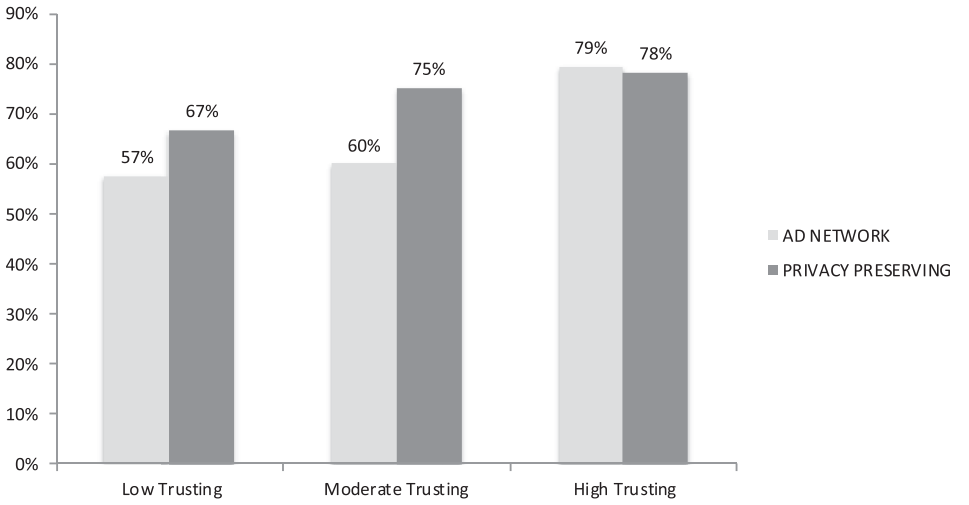

Figure 3: Percent of Respondents who Trust Player 2 by Respondent Trust

The decision of a partner, such as Player 2 in this experiment, to violate privacy norms by using an ad network impacts an individuals' willingness to engage. Put another way, violating privacy by using an ad network leads more consumers to not engage with a market actor, particularly for individuals with moderate and low institutional trust. This experiment undercuts the premise in the privacy paradox that consumers will not take privacy into consideration in market decisions.

DISCUSSION AND CONCLUSION

Contrary to the oft-repeated privacy paradox, the results show consumers retain privacy expectations after disclosing information and judge the sharing of information with third parties and the secondary use of information to be a violation of trust. Common secondary uses of information—such as selling consumer information to data aggregators and using an ad network—are considered on par with a security violation, such as outsider stealing information from a website—in terms of violating consumer trust. In addition, respecting privacy is important for consumers' economic behavior: the trust game experiment shows respondents are less willing to engage with a partner who violated privacy by utilizing an ad network as compared to one who used privacy preserving advertising, even when engagement is financially advantageous to the individual. Importantly, violating privacy by using an ad network leads more consumers to lose money, particularly for individuals with moderate and low institutional trust. Despite the argument that consumers relinquish privacy when disclosing information, consumers have specific expectations about how their information should be shared and used postdisclosure. In sum, these results undercut the privacy paradox as a concept, contradict the view that consumers willingly give up privacy when engaging with a website, and suggest that tracking for online marketing is considered a violation of consumer trust for websites. The study has theoretical and managerial implications.

Implications for Business Ethics

Theory

The substantive argument about privacy—or what does it mean to have privacy respected—has important implications in regards to the examination of privacy within business ethics. This study has suggested that individuals have privacy expectations, even when data is accessible or not controlled, and continues a line of scholarship supporting privacy as context-dependent norms within a community or a specific context. For business ethics, this shifts the research question from whether or not the handoff of information is adequately governed (Bowie and Jamal 2006) to what are the contextual norms of appropriate information flow for a given context. For example, if a scholar is studying education, the question centers on how technology used in an education system supports the information flows appropriate to that context. For business ethics, such an approach would suggest a new area of inquiry into the appropriate collection, aggregation, and use of information—of employees, of users, of consumers—within a given context within a firm.

In addition, the findings undercutting the privacy paradox broaden the scope of privacy inquiry, in that consumers have reasonable expectations of privacy even

after the information is disclosed or made public to others. For business ethics, firms take on many roles in gathering and using data previously disclosed or in public, including gathering license-plate readings, collecting and using location data, scraping disclosed information on social network sites, etc. If privacy norms prevail even after an individual has disclosed their information, business ethicists would need to identify the scope and type of responsibility of firms in regards to the privacy of employees, users, and consumers.

The current privacy paradox narrative limits the scope of corporate responsibility concerning consumer privacy. The privacy paradox implies firms have, at most, a negative duty to not hinder consumers in choosing preferences, since consumers are assumed to relinquish privacy upon the disclosure of information. However, the findings here suggest consumer facing firms have a positive duty to identify and respect privacy expectations of users, since privacy is valued similar to a security violation. This shift places privacy within the purview of corporate responsibility.

Empirical Research

The ethics of research that perpetuates the privacy paradox could easily be questioned based on this paper. Scholarship confirming the privacy paradox suggests the market behavior of consumers—such as disclosure of information or engagement with a website—is equated with consumers relinquishing privacy or somehow trading privacy away. This would be similar to framing the decision to work at a firm as the 'discrimination paradox,' whereby individuals claim to not approve of discrimination in surveys, but continue to work for firms that discriminate. Accordingly, labor economists would then study the discrimination paradox and explain why men and women continue to act in a paradoxical manner. However, we do not frame 'individuals who work at firms' as paradoxical; instead, we seek to understand why firms continue to undercut those reasonable expectations.

Framed in this manner, one can more clearly see the harm caused by research that perpetuates the privacy paradox and the associated guidance given to firms. When scholars equate disclosure, whether self-reported or actual disclosure to a researcher, with consumers not caring about and relinquishing privacy, the scholars perpetuate the myth that consumers have no reasonable expectations of privacy postdisclosure. This is why Kokolakis sees the danger in perpetuating the supposed privacy paradox: firms are encouraged to continue to collect and use consumer information due to scholars claiming a privacy paradox (Kokolakis 2017). This paper not only undercuts the privacy paradox, but would suggest that research perpetuating the privacy paradox through the mistaken framing of disclosure as proof of anti-privacy behavior is damaging as it gives license to firms to act in ways not in the interest of consumers. Researchers and firms may be mistakenly conflating market action—sharing information, entering into a transaction, becoming a customer, reading a website—as dispositive of acknowledging and accepting of the firms' information practices.

Implications for Public Policy

For public policy, the weaker version of the privacy paradox, where privacy is a preference traded in the market, is the basis for most US privacy regulations focused

on governing the point of disclosure with adequate notification and user choice. The privacy notices can say "we sell your data to the highest bidder," and as long as firms are accurate in their notice, US regulators, such as the FTC, are satisfied. Given the importance of privacy violations to consumer trust, this paper would suggest that a shift towards placing a positive obligation on consumer-facing firms to manage how consumer data is sold and is processed—a policy closer to the EU General Data Protection Regulation (GDPR)—would be likely in the future. Second, and more broadly, the results identify the importance of privacy violations to consumer trust as on par with security violations. Regulators such as the SEC, currently focused on security to maintain institutional trust, may need to consider privacy as a similarly important factor for consumer trust and their willingness to engage. If secondary uses of information are seen as akin to a security violation, a renewed effort to regulate secondary use of information could mirror the efforts around security.

Implications for Practice

The privacy paradox narrative gives companies license to ignore consumers' stated expectations in surveys and continue to track consumers and aggregate information. The reliance of industry on the privacy paradox to justify their marketing practices culminated in its inclusion in Mary Meeker's industry report (Meeker 2018) and a recent *Harvard Business Review* article advocating for the privacy paradox:

> There is indeed a privacy paradox, as even individuals who express concerns behave quite carelessly, engaging in uncensored or inappropriate self-disclosure, making a great deal of their digital footprint public, and allowing a wide range of external apps to access their data (Chamorro-Premuzic and Nahai 2017).

This paper undercuts the privacy paradox as a reasonable defense of privacy practices by firms. If consumers judge engagement with online marketing tactics, such as selling information to a data aggregator or using an ad network, to be a violation of privacy, then firms who transact with marketers online could face consumer backlash once the practices are known. Consumer-facing firms could create demand for solutions that limit the use of personal information shared, stored, and used for marketing, as has been recently studied (Holtrop et al. 2017; Schneider et al. 2017), particularly since research has illustrated the limits in effectiveness of personalized marketing tactics online (Lambrecht and Tucker 2013) and the limited value created by the online marketing ecosystem (Marotta, Zhang, and Acquisti 2017).

Finally, this study has implications for the relationship between firms and marketers. This study illustrated how websites are blamed for the tracking and secondary use of information by online marketers and data traffickers (Scholz 2019): consumer trust in a website was negatively impacted by dynamically targeting contacts and friends, and by selling information to a data aggregator. The interests of the larger online marketing ecosystem—which includes data aggregators, data brokers, and ad networks—to gather, aggregate, and sell personally identifiable information may not be aligned with the interests of firms to maintain consumer trust.

Limitations and Future Research

The concepts tested in this study are limited by how the theory was operationalized in the vignettes. And, the vignette factors in this study were determined by the author and based on theories of privacy. However, future research should examine other types and uses of information to identify the range of privacy violations equated to security violations by respondents. In addition, a limitation of this study is the reliance on MTurk for the sample. While the design addresses concerns with MTurk as a sample, the findings are not statistically generalizable to the US population. This study provides the relative importance of marketing uses of information in consumer trust, but does not provide statistical conclusions as to the amount of trust online, nor can the results be compared to other surveys measuring the amount of trust online. Future work could examine how the overall trust scores change across demographic groups and over time.

Conclusion

This paper undercuts the oft-reported privacy paradox and suggests users' privacy expectations are closely aligned with their stated preferences in surveys. Consumers have strong privacy norms about how consumer information is used for marketing, and respecting privacy impacts economic behavior. Firms have a corresponding positive obligation to understand privacy expectations of users and consumers.

SUPPLEMENTARY MATERIAL

To view supplementary material for this article, please visit https://doi.org/10.1017/beq.2019.24

ACKNOWLEDGEMENTS

I am grateful for support from the National Science Foundation under Grant No. 1649415. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–514.

Aguilar, Luis. 2014. "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus." Presented at the Cyber Risks and the Boardroom conference, New York Stock Exchange, June 10, 2014. http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

Allen, Anita L. 1988. *Uneasy Access: Privacy for Women in a Free Society*. New Jersey: Rowman & Littlefield.

Anderhub, Vital, Dirk Engelmann, and Werner Güth. 2002. "An Experimental Study of the Repeated Trust Game with Incomplete Information." *Journal of Economic Behavior & Organization* 48 (2): 197–216.

Arnold, Denis G. 2010. "Transnational Corporations and the Duty to Respect Basic Human Rights." *Business Ethics Quarterly* 20 (3): 371–399.

Auspurg, Katrin, Thomas Hinz, Stefan Liebig, and Carsten Sauer. 2014. "The Factorial Survey as a Method for Measuring Sensitive Issues." In *Improving Survey Methods: Lessons from Recent Research*, European Association of Methodology Series, edited by U. Engel, B. Jann, P. Lynn, A. Scherpenzeel, and P. Sturgis, 137–149. New York: Taylor & Francis.

Banerjee, Syagnik Sy, and Ruby Roy Dholakia. 2008. "Mobile Advertising: Does Location Based Advertising Work?" *International Journal of Mobile Marketing* 3 (2): 68–74.

Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States." *First Mondy* 11 (9).

Barth, Susanne, and Menno D.T. de Jong. 2017. "The Privacy Paradox—Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review." *Telematics and Informatics* 34 (7): 1038–1058.

Baruh, Lemi, Ekin Secinti, and Zeynep Cemalcilar. 2017. "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review." *Journal of Communication* 67 (1): 26–53.

Belanger, France, Janine S. Hiller, and Wanda J. Smith. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes." *The Journal of Strategic Information Systems* 11 (3): 245–270.

Berg, Joyce, John Dickhaut, and Kevin McCabe. 1995. "Trust, Reciprocity, and Social History." *Games and Economic Behavior* 10 (1): 122–142.

Bowie, Norman E., and Karim Jamal. 2006. "Privacy Rights on the Internet: Self-Regulation or Government Regulation?" *Business Ethics Quarterly* 16 (3): 323–342.

Chamorro-Premuzic, Tomas, and Nathalie Nahai. 2017. "Why We're So Hypocritical About Online Privacy." *Harvard Business Review*, May 1, 2017. https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy.

Cohen, Julie E. 2012. "What Privacy Is For." *Harvard Law Review* no. 126: 1904–1933.

Cropanzano, Russell, and Marie S. Mitchell. 2005. "Social Exchange Theory: An Interdisciplinary Review." *Journal of Management* 31 (6): 874–900.

Culnan, Mary J., and Robert J. Bies. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59 (2): 323–342.

Dienlin, Tobias, and Sabine Trepte. 2015. "Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors." *European Journal of Social Psychology* 45 (3): 285–297.

Dinev, Tamara, and Paul Hart. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17 (1): 61–80.

Dodd David. 2016. "The Most Effective Personalization Is Invisible." *customer THINK*, November 22, 2016. http://customerthink.com/the-most-effective-personalization-is-invisible/.

Donaldson, Thomas. 2003. "Values in Tension." In *Readings and Cases in International Management: A Cross-Cultural Perspective,* edited by D. C. Thomas, 133–140. Thousand Oaks, CA: Sage Publications.

Donaldson, Thomas, and Thomas W. Dunfee. 1994. "Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory." *Academy of Management Review* 19 (2): 252–284.

Donaldson, Thomas, and James P. Walsh. 2015. "Toward a Theory of Business." *Research in Organizational Behavior* no. 35: 181–207.

D'Souza, Giles, and Joseph E. Phelps. 2009. "The Privacy Paradox: The Case of Secondary Disclosure." *Review of Marketing Science* 7 (4): 1–29.

Englehardt, Steven, and Arvind Narayanan. 2016. "Online Tracking: A 1-Million-Site Measurement and Analysis." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

Etzioni, Amitai. 1999. *The Limits of Privacy*, Volume 5. New York: Basic Books.

Flavián, Carlos, and Miguel Guinalíu. 2006. "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site." *Industrial Management & Data Systems* 106 (5): 601–620.

Gabisch, Jason Aaron, and George R. Milne. 2014. "The Impact of Compensation on Information Ownership and Privacy Control." *Journal of Consumer Marketing* 31 (1): 13–26.

Ganong, Lawrence H., and Marilyn Coleman. 2006. "Multiple Segment Factorial Vignette Designs." *Journal of Marriage and Family* 68 (2): 455–468.

Glance David. 2018. "How Facebook Uses the 'Privacy Paradox' to Keep Users Sharing." *The Conversation*, April 15, 2018. http://theconversation.com/how-facebook-uses-the-privacy-paradox-to-keep-users-sharing-94779.

Guest Author. 2018. "The Privacy Paradox: The Right to Be Forgotten, But the Wish to Be Remembered." *Adweek*, September 3, 2018. https://www.adweek.com/digital/the-privacy-paradox-the-right-to-be-forgotten-but-the-wish-to-be-remembered/.

Hargittai, Eszter. 2010. "Facebook Privacy Settings: Who Cares?" *First Monday* 15 (8).

Holtrop, Niels, Jaap E. Wieringa, Maarten J. Gijsenberg, and Peter C. Verhoef. 2017. "No Future without the Past? Predicting Churn in the Face of Customer Privacy." *International Journal of Research in Marketing* 34 (1): 154–172.

Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Tom Lee. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment." *Mis Quarterly* 31 (1): 19–33.

Inness, Julie C. 1996. *Privacy, Intimacy, and Isolation*. New York: Oxford University Press.

Jasso, Guillermina. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments." *Sociological Methods & Research* 34 (3): 334–423.

Johnson, Michael D, and Fred Selnes. 2004. "Customer Portfolio Management: Toward a Dynamic Theory of Exchange Relationships." *Journal of Marketing* 68 (2): 1–17.

Johnson, Noel D, and Alexandra A Mislin. 2011. "Trust Games: A Meta-Analysis." *Journal of Economic Psychology* 32 (5): 865–889.

Kokolakis, Spyros. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64: 122–134.

Lacy, Lisa. 2018. "20 Takeaways From Mary Meeker's 2018 Internet Trends Report." *Adweek*, May 31, 2018. https://www.adweek.com/digital/20-takeaways-from-mary-meekers-2018-internet-trends-report/.

Lambrecht, Anja, and Catherine Tucker. 2013. "When Does Retargeting Work? Information Specificity in Online Advertising." *Journal of Marketing Research* 50 (5): 561–576.

Leon, Pedro Giovanni, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh. 2015. "Privacy and Behavioral Advertising: Towards Meeting Users' Preferences." *Symposium on Usable Privacy and Security (SOUPS),* July 22–24, 2015.

Madden, Mary. 2014. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Research Center*, November 12, 2014. https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

Malhotra, Deepak. 2004. "Trust and Reciprocity Decisions: The Differing Perspectives of Trustors and Trusted Parties." *Organizational Behavior and Human Decision Processes* 94 (2): 61–73.

Malhotra, Deepak, and J. Keith Murnighan. 2002. "The Effects of Contracts on Interpersonal Trust." *Administrative Science Quarterly* 47 (3): 534–559.

Marotta, Veronica, Kaifu Zhang, and Alessandro Acquisti. 2017. "The Welfare Impact of Targeted Advertising." Working paper.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. 2017. "Data Privacy: Effects on Customer and Firm Performance." *Journal of Marketing* 81(1): 36–58.

Martin, Kirsten. 2015. "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online." *Journal of Public Policy & Marketing* 34 (2): 210–227.

Martin, Kirsten. 2016. "Understanding Privacy Online: Development of a Social Contract Approach to Privacy." *Journal of Business Ethics* 137 (3): 551–569.

Martin, Kirsten. 2018. "The Penalty for Privacy Violations: How Privacy Violations Impact Trust Online." *Journal of Business Research* 82 (2018): 103–116.

Martin, Kirsten, and Helen Nissenbaum. 2017a. "Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables." *Columbia Science and Technology Law Review* 18 (Fall): 176–218.

Martin, Kirsten, and Helen Nissenbaum. 2017b. "Privacy Interests in Public Records: An Empirical Investigation." *Harvard Journal of Law and Technology* 31 (1). https://dx.doi.org/10.2139/ssrn.2875720.

Martin, Kirsten, and Katie Shilton. 2016. "Why Experience Matters to Privacy: How Context-based Experience Moderates Consumer Privacy Expectations for Mobile Applications." *Journal of the Association for Information Science and Technology* 67 (8): 1871–1882.

McKnight, D Harrison, Vivek Choudhury, and Charles Kacmar. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology." *Information Systems Research* 13 (3): 334–359.

Meeker, Mary. 2018. *Internet Trends Report 2018*. Kleiner Perkins, May 30, 2018. https://www.kleinerperkins.com/perspectives/internet-trends-report-2018.

Milne, George R., and Mary J. Culnan. 2004. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* 18 (3): 15–29.

Milne, George R., and Mary Ellen Gordon. 1993. "Direct Mail Privacy-Efficiency Trade-Offs within an Implied Social Contract Framework." *Journal of Public Policy & Marketing* 12 (2): 206–215.

Miyazaki, Anthony D., and Ana Fernandez. 2000. "Internet Privacy and Security: An Examination of Online Retailer Disclosures." *Journal of Public Policy & Marketing* 19 (1): 54–61.

Moore, Adam D. 2010. *Privacy Rights: Moral and Legal Foundations*. University Park, PA: Pennsylvania State University Press.

Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17 (5): 559–596.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–126.

Parent, William A. 1983. "A New Definition of Privacy for the Law." *Law and Philosophy* 2 (3): 305–338.

Pavlou, Paul A., and David Gefen. 2004. "Building Effective Online Marketplaces with Institution-Based Trust." *Information Systems Research* 15 (1): 37–59.

Pirson, Michael, Kirsten Martin, and Bidhan L. Parmar. 2017. "Formation of Stakeholder Trust in Business and the Role of Personal Values." *Journal of Business Ethics* 145 (1): 1–20.

Rainie, Lee, Sara Kiesler, Ruogu Kang, and Mary Madden. "Anonymity, Privacy, and Security Online." *Pew Research Center*, September 5, 2014. https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: University of North Carolina Press.

Rossi, Peter H., and Steven L. Nock. 1982. *Measuring Social Judgments: The Factorial Survey Approach*. Thousand Oaks, CA: Sage Publications.

Ruedy, Nicole E., Celia Moore, Francesca Gino, and Maurice E. Schweitzer. 2013. "The Cheater's High: The Unexpected Affective Benefits of Unethical Behavior." *Journal of Personality and Social Psychology* 105 (4): 531.

Schneider, Matthew J., Sharan Jagpal, Sachin Gupta, Shaobo Li, and Yan Yu. 2017. "Protecting Customer Privacy When Marketing with Second-Party Data." *International Journal of Research in Marketing* 34 (3): 593–603.

Schoeman, Ferdinand. 1984. "Privacy: Philosophical Dimensions." *American Philosophical Quarterly* 21 (3): 199–213.

Scholz, Lauren Henry. 2019. "Privacy Remedies." *Indiana Law Journal* 94 (forthcoming). https://ssrn.com/abstract=3159746.

Schumann, Jan H., Florian von Wangenheim, and Nicole Groene. 2014. "Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance among Users of Free Web Services." *Journal of Marketing* 78 (1): 59–75.

Sheehan, Kim Bartel, and Mariea Grubbs Hoy. 2000. "Dimensions of Privacy Concern among Online Consumers." *Journal of Public Policy & Marketing* 19 (1): 62–73.

Shue, Henry. 1996. *Basic Rights: Subsistence, Affluence, and US Foreign Policy*. Princeton, NJ: Princeton University Press.

Sirdeshmukh, Deepak, Jagdip Singh, and Barry Sabol. 2002. "Consumer Trust, Value, and Loyalty in Relational Exchanges." *Journal of Marketing* 66 (1): 15–37.

Stewart, David W. 2017. "A Comment on Privacy." *Journal of the Academy of Marketing Science* 45 (2): 156–159.

Strahilevitz, Lior Jacob, and Matthew B. Kugler. 2016. "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies* 45 (S2): S69–95.

Trimm, Trevor. 2016. "What Media Companies Don't Want You to Know about Ad Blockers." *Columbia Journalism Review*, June 29, 2016. http://www.cjr.org/opinion/ad_blockers_malware_new_york_times.php.

Tucker, Catherine E. 2012. "The Economics of Advertising and Privacy." *International Journal of Industrial Organization* 30 (3): 326–329.

Tufekci, Zeynep. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites." *Bulletin of Science, Technology & Society* 28 (1): 20–36.

Turow, Joseph, Michael Hennessy, and Nora Draper. 2015. *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, June 2015. Report from the Annenberg School for Communication, University of Pennsylvania. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." September 29, 2009. Available at SSRN: https://dx.doi.org/10.2139/ssrn.1478214.

Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising." In *Proceedings of the 8th Symposium on Usable Privacy and Security*. Association for Computer Machinery.

Vargo, Stephen L., and Robert F. Lusch. 2004. "Evolving to a New Dominant Logic for Marketing." *Journal of Marketing* 68 (1): 1–17.

Wallander, Lisa. 2009. "25 Years of Factorial Surveys in Sociology: A Review." *Social Science Research* 38 (3): 505–520.

Warren, Samuel D, and Louis D Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* no. 4: 193–220.

Westin, Alan. 2001. "Statement of Alan F. Westin." *Opinion Surveys: What Consumers Have to Say about Information Privacy*. Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce, U.S. House of Representatives, May 8, 2001.

Westin, Alan. 2003. "Social and Political Dimensions of Privacy." *Journal of Social Issues* 59 (2): 431–453.

Xu, Heng, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of Management Information Systems* 26 (3): 135–174.

Xu, Heng, Cheng Zhang, Pan Shi, and Peijian Song. 2009. "Exploring the Role of Overt vs. Covert Personalization Strategy in Privacy Calculus." *Academy of Management Proceedings*, no. 1.

Young, Alyson Leigh, and Anabel Quan-Haase. 2013. "Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited." *Information, Communication & Society* 16 (4): 479–500.

APPENDIX A
CONTROL VARIABLES

Variable	Options/Item	Values
Gender	Male	1
	Female	2
Age	Under 18	1
	18-24	2
	25-34	3
	35-44	4
	45-54	5
	55-64	6
	65 +	7
40 Vignettes	I trust this website.	-100...+100
Knowledge Internet:	I don't know any technical details	1

Appendix A: continued

Variable	Options/Item	Values
How would you judge your knowledge of the technical aspects that make the Internet work?	I have a vague idea of the technical details	2
	I have a good idea of the technical details	3
	I am very knowledgeable	4
	I am an expert	5
Privacy Concern	I am concerned that online companies are collecting too much personal information about me.	-100...+100
Trust in Websites	In general, I trust websites.	-100...+100
Coding Experience:	I have coded in too many languages to count	1
How many programming languages have you used for coding?	I have coded in several (2-4) programming languages	2
	I have coded in one programming language	3
	I have coded but do not remember the language	4
	None - I have never coded	5
Privacy Important	In general, I believe privacy is important	-100...+100

. . .

Kirsten Martin is an associate professor of strategic management and public policy at the George Washington University School of Business. She researches privacy, technology, and corporate responsibility. She has written about privacy and the ethics of technology in academic journals across disciplines (*Journal of Business Ethics, Harvard Journal of Law and Technology, Journal of Legal Studies, Washington University Law Review, Journal of Business Research,* etc.) as well as practitioner publications such as *MISQ Executive*. She is the Technology and Business Ethics section editor for the *Journal of Business Ethics* and the recipient of three NSF grants for her work on privacy, technology, and ethics. Martin is also a member of the advisory board for the *Future Privacy Forum* and a fellow at the *Business Roundtable Institute for Corporate Ethics* for her work on stakeholder theory and trust. She is regularly asked to speak on privacy and the ethics of big data, including her 2018 TEDx talk. She earned her BS Engineering from the University of Michigan and her MBA and PhD from the University of Virginia's Darden School of Business.