Marketing Science Institute Working Paper Series 2021

Report No. 21-118

No to Facebook but Yes to Amazon: A Multi-method Investigation of Consumer Response to Privacy Violations

Chi Tran, Brandon J. Reich and Hong Yuan

No to Facebook but Yes to Amazon: A Multi-method Investigation of Consumer Response to Privacy Violations

Submission Date: February 9, 2021

Chi Tran
Ph.D. Candidate
Lundquist College of Business
University of Oregon
1208 University of Oregon
Eugene, OR 97403
email: ctran4@uoregon.edu

Brandon J. Reich
Assistant Professor in Marketing
Portland State University
The School of Business
615 SW Harrison Street
Portland, OR 97201
email: breich@pdx.edu
phone: 503-725-3509

Hong Yuan
Richard P. Booth Associate Professor and Research Scholar
Lundquist College of Business
University of Oregon
1208 University of Oregon
Eugene, OR 97403
email: hongy@uoregon.edu
phone: 541-346-3196

In April 2019, Facebook's CEO Mark Zuckerberg declared to the world that "The future is private" and that the world's largest social media platform would be pivoting to a privacy-focused strategy (Nivea 2019). This denotes a significant shift from his own declaration in 2010 that privacy was an obsolete social norm of the past (Kirkpatrick 2010). Other companies have followed suit, changing their regard for privacy from a burdensome cost for risk management (Bamberger and Mulligan 2010) to a growing recognition of privacy as a potential source of competitive advantage. Apple, for example, recently released a major ad campaign with the simple tagline: "Privacy. That's iPhone." (Wuerthele 2019).

Clearly privacy is more important to consumers than ever before (Krishna 2020), in part due to marketers' own exploitation of consumer data over the past decade (Benes 2018). More surprisingly, while consumers report unprecedented levels of privacy concerns (PwC 2017) and lack of control over their personal information (Pew 2019), they continue to patronize the products and services of many of the companies that routinely violate their privacy. The literature has dubbed this the "privacy paradox" (Aguirre et al. 2014; Awad and Krishnan 2006; Krasnova et al. 2010), a phenomenon whereby consumers self-report strong privacy concerns but often do not behave accordingly. For instance, consumers continue to tolerate intrusive privacy practices by companies such as Amazon (Paul 2020) and Google (MacMillan and McMillan 2018), while Facebook's similarly intrusive privacy violations have produced fierce consumer backlash (Shane 2018).

For all its importance to modern consumption and marketing, a consensus definition of consumer privacy remains elusive (Acquisti, Taylor, and Wagman 2016; Martin and Murphy 2017), in part because privacy is a constantly evolving and "essentially contested" construct (Mulligan, Koopman, and Doty 2016). For marketing practitioners, perhaps even more important

than understanding what privacy means is clarifying what a privacy violation entails in a contemporary digital landscape (MacInnis et al. 2020). Moreover, although the privacy paradox is well-documented, its underlying process and operationalization remain poorly understood (Acquisti, Brandimarte, and Loewenstein 2020; Krasnova et al. 2010).

Motivated by this dearth of knowledge, the current research has two core aims. First, we seek to clarify the construct of privacy violation from a consumer perspective. Using an established construct development methodology, we establish that consumers perceive three privacy violation types reflecting a linear increase in severity: *recording* (i.e. merely observing and storing consumers' personal information), *targeting* (i.e., using consumers' information for targeted advertisements), and *sharing* (i.e., sharing consumers' information with a third party). This conceptualization in turn facilitates our second aim, explaining the privacy paradox by reconciling seemingly contradictory consumer responses to differing privacy situations.

Synthesizing literatures pertaining to consumer privacy (Martin and Murphy 2017; Smith, Dinev, and Xu 2011), control (Deci and Ryan 2000; Skinner 1996) and coping (Dweck 2000), we theorize that more severe privacy violations reduce consumers' resource control (i.e., their subjective control over a valued resource; Fast et al. 2009). We predict that consumers will cope with this loss of control differently depending on marketplace conditions. When situation controllability is high (i.e., one's behavior does not seem constrained by the external situation; Ajzen 2002) regaining resource control seems feasible, and consumers will therefore engage in active coping (e.g., through brand switching; Schiele and Venkatesh 2016). Conversely, when regaining resource control is perceived as impossible (i.e., when situation controllability is low), a sense of helplessness inhibits such control-reclaiming behaviors and consumers cope more passively (Dweck 2000).

In a market setting, this crucial boundary condition may manifest as the variability of privacy practices in an industry. That is, we expect a severe (vs. moderate) privacy violation to prompt greater control-reclaiming behaviors, only when the violating company operates in an industry with high variability of privacy practices. This is because, in this market context, regaining control over one's information still seems possible. However, in a homogenous industry in which companies share a standardized privacy practice, consumers are unlikely to engage in control-reclaiming behaviors regardless of violation severity because regaining control seems impossible. If correct, our theorizing parsimoniously explains the otherwise opaque privacy paradox and its most noteworthy marketplace manifestations, such as consumers' backlash against Facebook but complacency with Amazon or Google.

The remainder of this manuscript proceeds as follows. First, we present a rigorous review of several literatures spanning consumer privacy, control, and coping, leading to our predictions around the meaning of privacy violation and when it translates into consumer action. We then use a multi-method approach to test this conceptualization across five studies. Using a combination of interview and survey designs, Study 1 first clarifies the construct of privacy violation from a consumer perspective, uncovering and confirming three increasingly severe violation types: *recording*, *targeting* and *sharing* of personal information. We then use this conceptualization to shed light on the privacy paradox. Using a between-participants experiment (Study 2), we test an industry-level manifestation of situation controllability—variability in privacy practices (henceforth "industry variability")—that helps explain differential consumer responses to otherwise equivalent privacy violations across companies. In Study 3, by manipulating violation type and resource control in a full-factorial design, we directly examine the role of resource control as the mechanism driving the relationship between privacy violations

and consumer response. In an experiment utilizing consumers' realistic experience with a novel mobile app, Study 4 then demonstrates this mechanism using tests of mediation and its interaction with industry variability on consumers' response towards different violation types. Thus, our complete conceptual model is tested in Study 4. Finally, using text analysis of scraped Twitter data, Study 5 tests these effects in a naturalistic setting.

THEORETICAL FRAMEWORK

Consumer Privacy and Privacy Violation

Privacy has traditionally been defined as a right "to be left alone" (Brandeis and Warren 1890), specifically with reference to one's own physical space. Due to recent shifts in technology, contemporary definitions of consumer privacy often imply information privacy (Goodwin 1991), especially in an online consumption domain. Indeed, the "information age" has created such widespread consumer demand for information privacy that it is sometimes regarded as a commodity that could be regulated through a market structure (Acquisti, Taylor, and Wagman 2016; Smith, Dinev, and Xu 2011). In theory, this suggests that consumers may willingly exchange privacy and personal information for access to products and services.

Despite this theoretical guidance and the growing attention paid to consumer privacy, there remains a lack of consensus as to what constitutes a privacy violation (Martin and Murphy 2017). How should marketers tread this evolving consumer landscape? On the one hand, the advanced use of information has significantly improved marketers' precision in understanding and reaching consumers. However, advancing a data-driven, consumer-focused strategy may also violate consumers' privacy. As the need to balance this tension grows, so too does the need to understand what privacy violation means from a consumer perspective (MacInnis et al. 2020).

Notably, the marketing literature has provided some guidance as to conceptualizing privacy violation. For instance, Nill and Aalberts (2014) define it as unwanted marketing communications, highly targeted advertisement, and secretive online tracking. This approach focuses on companies' use of consumer data without consent. While providing a useful foundation, this definition does little to address the increasingly nuanced use of consumer data in the current digital environment. Is seeing an ad about a product one might like "unwanted?" How targeted is "highly targeted?" Would consumers consider an advertisement specifically targeted at them a "privacy violation?" These questions remain open, portending a lack of clarity with respect to the concept of privacy violation from a consumer perspective.

Addressing this gap, we investigate how consumers conceptualize privacy violations. Past work suggests that a violation is seen as severe only when a large amount of information is collected or when the type of information is highly sensitive (Phelps, Nowak, and Ferrell 2000). Although these criteria may contribute to perceived privacy violation, we focus on an often-overlooked component. That is, rather than the quantity or quality of information collected, our research suggests that consumers emphasize what the company *does* with their information in determining whether and to what extent a privacy violation has occurred. Specifically, using a combination of interview, survey, and experimental methodologies, our results reveal three privacy violation types—*recording*, *targeting*, and *sharing*—that explain the bulk of variation in perceived privacy violations and represent a linear increase in severity.

We further propose and show that these violation types differentially affect consumer response *because* they represent increasing levels of privacy violation. Given that consumer privacy is often defined in terms of consumers' perceived control over the collection and use of their personal information (Goodwin 1991), it follows that what companies do with consumers'

data influences perceptions of violation severity because it affects the control consumers feel they have over their information. Across these three violation types, *recording* represents the least amount of usage or manipulation over consumer data. Conversely, *targeting* and *sharing* both involve further manipulation and exploitation of such data, suggesting that consumers likely perceive these violation types as more severe.

Interestingly, *targeting* and *sharing* are often confounded and labeled "personalization" in the marketing literature (Vesanen and Raulas 2006). For example, behavioral targeting is defined as utilizing consumer behavioral data from multiple sources to deliver personalized ads to users (Summers, Smith, and Reczek 2016). Likewise, adaptive personalization involves constantly updating user preference using data shared among platforms and systems to deliver targeted ads to consumers (Chung, Wedel, and Rust 2016). These examples suggest that delivering targeted recommendations and customizing ads by sharing consumer data with a third-party would both be labeled "personalization" according to current conceptualizations.

However, gossip theory (Martin, Borah, and Palmatier 2017) suggests that consumers may perceive *sharing* to be more intrusive than *targeting*. In social relationships, people feel reduced control over their personal information (and in turn feel more vulnerable) when it is shared with another party (Wert and Salovey 2004). When they learn that they are the subject of gossip, for instance, most people react negatively because their privacy has been severely violated (Baumeister, Zhang, and Vohs 2004). In addition, *sharing* is fundamentally different from *targeting* and *recording* as it involves secondary use of consumer data, depriving consumers of their control over their information and exposing them to additional risks (Acquisti, Brandimarte, and Loewenstein 2020). Consistent with this theoretical perspective, we expect that consumers will perceive *sharing* (vs. *targeting*) as a more severe privacy violation

because it reduces their perceived control over their own information, and both will be perceived as more severe than *recording* for this same reason.

Resource Control, Situation Controllability, and Coping

We have thus far conceptualized privacy violation in terms of consumers' perceived control over their personal information, a valued resource. Much like parallel constructs, such as psychological power—the asymmetric control over valued resources in social relations (Fast et al. 2009) —lacking control is generally considered aversive and the literature suggests that consumers often try to regain control when it is threatened or lost (Whitson and Galinsky 2008). This suggests that, as the severity of privacy violation increases, a decrease in resource control leads to an increased likelihood that consumers will attempt to actively regain control. Yet, a privacy paradox has been documented (Norberg, Horne, and Horne 2007; Sheehan and Hoy 1999) whereby consumers sometimes do not respond appropriately following a privacy violation.

To resolve these conflicting theoretical perspectives, we draw from literatures on self-determination and coping. Self-determination theory corroborates our prediction that individuals cope with threats to control by engaging in control-reclaiming behaviors (Deci and Ryan 2000), such as domain-specific attempts to solve a problem (e.g., through brand selection; Schiele and Venkatesh 2016) or as generalized self-affirmations of one's overall sense of control (e.g., through verbal expressions; Thimm, Rademacher, and Kruse 1995). Indeed, we expect this type of active coping response in situations in which regaining control seems possible (i.e., when situation controllability is high). However, the coping literature adds nuance and suggests that consumers may respond more passively in situations in which regaining control seems impossible (i.e., when situation controllability is low; Skinner and Zimmer-Gembeck 2011). In such cases, a sense of helplessness inhibits control-reclaiming behaviors and no action is taken

(Dweck 2000; Skinner 1996), sometimes referred to in a consumer privacy context as a "digital resignation" (Draper and Turow 2019). In a marketplace setting, we propose that situation controllability may manifest as an industry-level characteristic that helps explain the privacy paradox. Industry variability—the amount of variability between companies within an industry in terms of their privacy practices—may indeed explain why severe (vs. moderate) privacy violations prompt consumer action in some market contexts (e.g., social media; Hajli and Lin 2016) and not others (e.g., online retail; Grosso et al. 2020). This actual marketplace condition, though rarely examined in the literature, has important implications for both marketing practice and theoretical understanding of consumer privacy.

In sum, we predict that a severe (vs. moderate) privacy violation will prompt greater control-reclaiming behaviors, but only when the violating company operates in an industry with high variability of privacy practices. This is because, in this market context, regaining resource control still seems possible (i.e., situation controllability is high). However, in a homogenous industry in which companies share a standardized privacy practice, consumers are unlikely to do so regardless of violation severity because regaining control seems impossible (i.e., situation controllability is low). Figure 1 (Tables and Figures follow Reference throughout) summarizes our conceptual framework and constructs.

STUDY 1

Study 1, motivated by in-depth interviews with privacy experts, aimed to explore and develop the construct of privacy violation from a consumer perspective. The interviews allowed us to explore the state of the literature in adjacent fields. For the main study, we then used a

scenario-based survey to identify common themes among actual privacy incidents resulting in the conceptualization of three violation types.

In-depth interviews

We interviewed two privacy experts in law and public policy to uncover the current state of literature around privacy in the respondents' respective fields. We employed a semi-structured technique (Irvine, Drew, and Sainsbury 2013), posing pre-determined open-ended questions while allowing for flexibility and spontaneous follow-ups. An extensive, iterative review of the transcripts revealed three core themes across both interviewees: (1) consumer privacy is an evolving and underdeveloped construct, exposing consumers to risks of violation, (2) future research should assess consumer privacy scenarios to identify dimensions of the construct, and (3) contextual factors (i.e., those beyond individual characteristics) play an important role in privacy behaviors. As consumers, however, these interviewees expressed a decision to stop or reduce their usage on certain platforms (e.g., Facebook) but continued to support others (e.g., Google or Amazon), even though they admitted that these platforms were equally intrusive. As one interviewee stated, "I deleted my Facebook after I did some research on how intrusive it is. But I have to admit I have two [Amazon Echo] Dots at home that I use daily, although they're probably listening to everything we say." This shows that even privacy experts are subject to the privacy paradox as consumers, further motivating us to delve into the granularity of privacy violations in the current climate of consumer data.

Method

Study 1 utilized several actual instances of consumer privacy violations that have occurred in the past ten years. Participants (N = 139 US residents; $M_{Age} = 36.32$, $SD_{Age} = 11.70$; 41.01% female) were recruited from Amazon's Mechanical Turk (MTurk) and were first asked

to provide their own privacy definition in a text box. Next, they were presented with twelve scenarios, each presented on its own page and in randomized order (see Table 1 for scenarios; Tables and Figures follow Reference throughout). To create these scenarios, we collected a list of privacy incidents reported in the major business press in the past ten years (e.g., The Wall Street Journal, Business Insider, Forbes, etc.) using the business press database Factiva. We excluded incidents of data breaches in which both the company and consumer were victims and filtered out incidents caused by personal errors. We then selected scenarios that garnered substantial media interest at the time and adapted them into short descriptions without mentioning specific companies' names. Participants' self-reported privacy definition was piped back into a display under each scenario for reference, and participants rated their perceived level of privacy violation for each using a single item: "This action is…" (1 = *Not at all a privacy violation*; 7 = *An extreme privacy violation*).

Results

A Principal Component Analysis (PCA) with Varimax rotation (see Table 1) found that the twelve ratings converged into three components with step levels of perceived privacy violation. Component 1 (*recording*; M = 3.38, SD = 1.30) consisted of scenarios in which companies merely collected consumer information (e.g., "CCTV in the supermarket aisle that tracks customers' activity in-store."). Component 2 (*targeting*; M = 5.16, SD = 1.21) included situations in which companies used consumer information for targeting purposes (e.g., "A retailer uses a customer's purchase history to predict that a customer is pregnant and send pregnancy advertisements to her address."). Component 3 (*sharing*; M = 6.12, SD = 1.06) consisted of actions involving sharing information with third parties (e.g., "A social media app allows third-party developers access to users' data.").

A follow-up repeated-measures ANOVA comparing the composite means of these components suggested a significant omnibus difference (Hyunh-Feldt $F(1.77, 243.67) = 262.28$, $p < .001$), and planned polynomial contrasts showed a significant linear trend ($F(1, 138) = 376.36$, $p < .001$). This suggests that consumers perceive progressively increasing levels of privacy violation depending on whether the violation type is *recording*, *targeting* or *sharing*. We also replicated these results in an identical survey among 113 undergraduate students ($M_{Age} = 25.85$, $SD_{Age} = 7.32$; 67.0% female), suggesting that the component structure is robust across populations; see Appendix A for full replication results).

Discussion

This study provided initial evidence that consumers may perceive distinct levels of privacy violation depending on what companies do with their information, increasing progressively in a linear trend across *recording*, *targeting* and *sharing* violation types. Our findings also highlight the distinction between *sharing* and *targeting*, concepts which extant literature has traditionally confounded. In Study 2, we confirm this conceptualization with an experimental design and test our control-based explanation for the privacy paradox.

STUDY 2

Study 2 aimed to replicate and extend the findings of Study 1 using a controlled experimental design among fictitious brands. In addition, Study 2 examined the roles of violation type and situation controllability (operationalized as industry variability) in consumer control-reclaiming behavior (operationalized as brand switching). We first conducted a pretest to confirm the three violation types uncovered in Study 1. The main study then followed and utilized a 3 (violation type: *recording, targeting, sharing*) × 2 (industry variability: low, high)

full-factorial design. We expected increased control-reclaiming behavior in response to a *sharing* (vs. *targeting* or *recording*) privacy violation when the industry is highly varied in its privacy practice. However, this effect should be mitigated when the industry is standardized.

Pretest

The pretest recruited 302 US residents from MTurk (N = 287 after attention check exclusions, $M_{Age} = 38.5$, $SD_{Age} = 12.48$; 50.4% female) to participate in a 3 (violation type: *recording, targeting, sharing*) × 2 (industry category: online shopping, social media) between-participants design. We asked consumers to participate in a familiar online environment without mentioning specific companies' names. This permitted us to rule out potential confounds with regards to pre-existing attitudes towards the focal company. Industry category was manipulated to enhance external validity, with the expectation that the effect of violation type on violation severity follows the same pattern across industry categories.

Procedure. Participants in the online shopping (social media) category condition were asked to imagine that they were returning to an online retailer (a social media platform) that they had used before. Participants then saw a small pop-up window explaining that the company's cookies policy permitted collection of information regarding websites they visited, duration of their visit, and their IP address (see Appendix D). This created a realistic, common consumer situation while holding constant the type and amount of information collected across conditions.

In the *recording* condition, the pop-up window stated that their information would be used to improve their experience but not used for advertisements or shared with third-parties. In the *targeting* (*sharing*) conditions, the information *would* be used to deliver targeted ads (shared with third-parties). To hold constant participants' perceived benefits to the company, in all conditions the scenario mentioned that the company would gain $10 per user annually from this

practice. Participants then rated perceived privacy violation with a four-item scale (α = .87) adapted from Krasnova et al. (2010; see Appendix C for scale items used in all studies). Lastly, an attention check asked participants to "Select Strongly Disagree for this question."

Results. A 3 (violation type) × 2 (industry category) factorial ANOVA on perceived privacy violation (see Figure 2 for means and standard deviations) showed only a significant main effect of violation type ($F(2, 281) = 3.00$, $p = .05$; other ps > .21). We therefore collapsed and controlled for industry category in subsequent analyses. Planned polynomial contrasts confirmed Study 1's results via a significant linear trend of violation type on privacy violation ($F(1, 281) = 4.26$, $p = .02$), but no significant quadratic trend ($p = .86$), such that *recording*, *targeting*, and *sharing* represented increasingly severe privacy violations regardless of industry category. We next use this conceptualization to test the impacts of these violation types on control-reclaiming behaviors in the main study.

Method

Study 2 used a 3 (violation type: *recording*, *targeting*, *sharing*) × 2 (industry variability: low, high) full-factorial design with 548 US residents recruited from MTurk (N = 385 after attention check exclusions, $M_{Age} = 38.94$, $SD_{Age} = 12.26$; 51.70% female). Participants were given information about "Industry X," containing four companies (A, B, C, and D) and were asked to imagine themselves as current customers of "Company A," the market leader. In the low (high) variability condition, all companies in Industry X used consumer data in the same way (different ways; see Appendix B). As in the pretest, participants in the *recording* (*targeting*) [*sharing*] condition then saw a pop-up detailing Company A's cookies policy of merely recording consumers' data (using consumers' personal data to deliver targeted ads) [sharing consumers' data with third-parties].

Brand switching, the core dependent variable, was operationalized using both a dichotomous and continuous item. Participants first indicated whether they would continue onto Company A's website (0) or switch to another brand (1). They then indicated how strongly they felt about their choice on a continuous scale (1 = *Strongly confident to continue with Company A*; 13 = *Strongly confident to switch to another company*). The two items were highly correlated (r = .90) and thus standardized and averaged to form an index of brand switching. Conducting all analyses in Studies 2 – 4 using each individual switching item (rather than the combined index) did not change the direction or significance of results (see Appendix E). We therefore retain the more robust index measure in our analyses.

To check if the variability manipulation was successful, we asked participants to rate "How much variety is there in privacy policies of companies in Industry X" on a seven-point scale (1 = *All have the same privacy policies*; 7 = *All have different privacy policies*). To ensure that participants did not think that the company benefited differently depending on violation type, participants were also asked to rate the extent to which the company's data practice benefited the company (vs. consumers) on a scale from 1 (*primarily benefiting Company A*) to 7 (*primarily benefiting consumers*). Lastly, participants completed an attention check regarding Company A's cookies policy, followed by demographic questions.

Results

Manipulation checks. We first conducted a 3 (violation type) × 2 (industry variability) ANOVA on perceived privacy violation. Results showed only a significant main effect of violation type on privacy violation ($F(2, 379) = 4.46$, $p = .01$, other ps > .16; $M_{Recording} = 3.97$, $SD_{Recording} = 0.62$, $M_{Targeting} = 4.19$, $SD_{Targeting} = 0.86$, $M_{Sharing} = 4.26$, $SD_{Sharing} = 0.83$). A parallel ANOVA on the variability check revealed the expected main effect of industry variability (F(1,

379) = 803.69, $p < .001$, $M_{High\ Variability} = 6.43$, $SD_{High\ Variability} = 1.06$, $M_{Low\ Variability} = 1.99$, $SD_{Low\ Variability} = 1.95$). Surprisingly, we did observe a significant main effect of violation type ($F(2, 379) = 3.88$, $p = .02$) and a significant violation type × industry variability interaction on the variability check ($F(2, 379) = 4.02$, $p = .02$). However, because the main effect of variability remained significant at all three levels of violation type (ps < .001), we disregard this interaction and conclude that our manipulations were successful. Lastly, a similar ANOVA on perceived company benefit revealed no significant main or interaction effects (ps > .15) confirming that participants did not perceive differential benefits for the company across conditions.

Main effects and interaction. To test our core predictions, we conducted a 3 (violation type) × 2 (industry variability) factorial ANOVA on the switching index. Consistent with our previous findings and theorizing, results showed a significant main effect of violation type on switching behavior ($F(2, 379) = 20.51$, $p < .01$). Planned contrasts showed that those in the *sharing* condition ($M_{Sharing} = 0.39$, $SD_{Sharing} = 1.14$) were significantly more likely to switch than those in the *targeting* ($M_{Targeting} = -0.18$, $SD_{Targeting} = .86$, $p < .001$) and *recording* conditions ($M_{Recording} = -0.29$, $SD_{Recording} = 0.79$, $p < .001$). Switching likelihood did not significantly differ between the *recording* and *targeting* conditions ($p = .60$). There was also a significant main effect of industry variability on switching behavior such that those in the high (vs. low) variability condition were much more likely to switch ($F(2, 379) = 13.23$, $p < .001$, $M_{High\ Variability} = 0.18$, $SD_{High\ Variability} = 1.08$, $M_{Low\ Variability} = -0.20$, $SD_{Low\ Variability} = 0.81$).

Importantly, these main effects were qualified by a significant two-way interaction ($F(2, 379) = 7.42$, $p = .001$, Figure 3). Planned contrasts revealed that, in the high industry variability condition, participants were significantly more likely to switch brands in the *sharing* condition ($M_{Sharing} = 0.76$, $SD_{Sharing} = 1.14$) as compared to the *targeting* ($M_{Targeting} = 0.06$, $SD_{Targeting} =$

0.96, $p < .001$) or *recording* condition ($M_{Recording} = -0.37$, $SD_{Recording} = 0.80$, $p < .001$). Although switching was descriptively more likely in the *targeting* (vs. *recording*) condition, this difference did not reach statistical significance ($p = .13$). However, a follow-up polynomial contrast revealed a significant linear trend within the high variability condition ($F(1, 196) = 35.84$, $p < .001$). Conversely, and as theorized, in the low industry variability condition, violation type had no effect on participants' switching behavior ($p = .11$).

Discussion

Findings in Study 2 further support our theorizing regarding the nuanced effects of companies' usage of consumer data on behavioral responses. Results affirmed that *sharing* (vs. *targeting* and *recording*) consumer data is a more egregious privacy violation and increases switching behavior. This study also demonstrates an industry-level factor that moderates this relationship and may explain the privacy paradox. If the industry has low variability in privacy practice, then different levels of privacy violation may not translate into switching behavior as consumers may feel a sense of digital resignation (Draper and Turow 2019). That is, in standardized industries (e.g., online retail), situation controllability is low and a sense of helplessness therefore inhibits consumers' willingness to actively reclaim control regardless of violation severity. In other industries with more varied privacy practice (e.g., social media), consumers are more likely to engage in control-reclaiming behavior because it still seems possible for them to reclaim control (i.e., situation controllability is high). Having established the three violation types, subsequent studies focus more narrowly on the distinction between *targeting* and *sharing* to provide a more conservative and streamlined test of the underlying control-based mechanism. This also more accurately reflects most market situations in which

recording is ubiquitous (Acquisti, Brandimarte, and Loewenstein 2020) but companies differ in terms of whether consumer data is used for *targeting* or *sharing* with third parties.

STUDY 3

Study 3 further dissects the differences between *targeting* and *sharing*, and tests the underlying role of resource control in consumers' response to privacy violation. Our framework asserts that consumer response to privacy violations are rooted in their drive to reclaim lost control over their personal information. If our theorizing is correct, then priming consumers with high (vs. low) resource control should satisfy this need and therefore inhibit the compensatory path that consumers otherwise take when their privacy is violated in a highly variable industry.

Method

This study recruited 220 business students (N = 187 after attention check exclusions, $M_{Age} = 20.78$, $SD_{Age} = 1.57$; 62.60% female) at a public university who participated in exchange for course credit. Consistent with our previous studies, only US residents were recruited as privacy norms and tolerance could vary widely across cultures (Markos, Milne, and Peltier 2017). Upon arriving at a computer lab, participants were randomly assigned to conditions in a 2 (resource control: low, high) × 2 (violation type: *targeting*, *sharing*) between-participants experiment and were told that the study consisted of two unrelated parts. In the first part, they completed a resource control manipulation task under the disguise of a business situation, detailed on a piece of paper preset for them by a research assistant. Because resource control is a necessary but not sufficient precursor to power (Rucker, Galinsky, and Dubois 2012), we adapted McAlister, Bazerman, and Fader's (1986) channel negotiation task to directly manipulate resource control in particular rather than power more generally.

The manipulation asked participants to imagine themselves in a business negotiation scenario in which they were a manager tasked with purchasing a piece of equipment with a $100,000 budget. In the high (low) resource control condition, participants were informed that the piece of equipment was in extremely low (high) demand and that there were many suppliers (competitors) in the market. Thus, in the high (low) resource control condition, the scenario created a resource imbalance in (against) participants' favor. Participants then were told that they received a quote for $120,000, and asked to write their counter offer on that piece of paper. This offer amount was used as a check on the resource control manipulation. As an additional manipulation check, on a computer screen, participants were asked to rate their overall sense of control over the resources involved on a two-item, five-point Likert scale (r = .70, Ajzen 2002).

The second part of the study, also completed on a computer screen, proceeded similarly to Study 2. Participants were provided with information about Industry X (containing four companies) and were told they were current customers of Company A. In the *sharing* (*targeting*) condition, a cookies pop-up explained that Company A was collecting and using their information to share with a third party (deliver targeted ads). Participants were then presented with the same two-item switching index (r = .82), containing both a dichotomous and continuous item. Next, participants completed an attention check item regarding Company A's cookies policy, and were debriefed and thanked for their participation. After participants exited the lab, a research assistant collected and recorded their responses to the first task.

Results

Manipulation checks. As found by McAlister, Bazerman, and Fader (1986), we expected that those in the high (low) resource control condition would report feeling more (less) control and offer a significantly lower (higher) amount. We conducted a pair of 2 (resource control) × 2

(violation type) factorial ANOVAs on offer amount and the perceived control measure and found only a main effect of resource control on both manipulation checks. On average, those in the high resource control condition were willing to offer less than those in the low resource control condition ($F(1, 183) = 24.90$, $p < .001$, $M_{\text{High Control}} = \$80{,}521$, $SD_{\text{High Control}} = 13{,}968$, $M_{\text{Low Control}} = \$109{,}274$, $SD_{\text{Low Control}} = 52{,}644$). They also reported feeling significantly more control ($F(1, 183) = 112.03$, $p < .001$, $M_{\text{High Control}} = 3.72$, $SD_{\text{High Control}} = 0.90$, $M_{\text{Low Control}} = 2.29$, $SD_{\text{Low Control}} = 0.93$). There was no significant main effect of violation type or interaction on either measure (all *p*s >.51). These results suggest that the resource control manipulation was successful.

Main effects and interaction. A 2 (resource control) × 2 (violation type) factorial ANOVA on the switching index revealed a main effect of violation type such that participants in the *sharing* (vs. *targeting*) condition were significantly more likely to switch ($F(1, 183) = 10.77$, $p = .001$, $M_{Sharing} = 0.25$, $SD_{Sharing} = 1.04$, $M_{Targeting} = -0.20$, $SD_{Targeting} = 0.84$), but no main effect of resource control ($p = .45$) was observed. Importantly, results also indicated a significant two-way interaction ($F(1, 183) = 4.35$, $p = .04$, Figure 4). Planned contrasts showed that in the low resource control condition, results mirrored those of our prior studies such that participants were more likely to switch in the *sharing* (vs. *targeting*) condition ($M_{Sharing} = 0.44$, $SD_{Sharing} = 1.04$, $M_{Targeting} = -0.29$, $SD_{Targeting} = 0.76$, $p < .001$). However, in the high resource control condition, the effect was eliminated ($M_{Sharing} = 0.05$, $SD_{Sharing} = 0.99$, $M_{Targeting} = -0.11$, $SD_{Targeting} = 0.91$, $p = .40$).

Discussion

Findings from Study 3 reaffirm our conceptual distinction between *targeting* and *sharing*, suggesting that consumers might consider the latter (vs. former) type of privacy violation to be more severe. Results also support our theorizing that consumers respond to privacy violations

with attempts to regain resource control when market factors provide situation controllability. When consumers' resource control was primed from a different source, their need to reclaim control through brand switching was eliminated. Our findings therefore establish that consumers' reaction to privacy violations is primarily rooted in their need to reclaim lost control. This mechanism helps explain past work showing that when consumers are given options to control their information on a technological platform, they surrender more personal information (Brandimarte, Acquisti, and Loewenstein 2012) or become less guarded towards personalized marketing practice (Tucker 2014). In Study 4, we provide an alternative test of this mechanism in a more ecologically valid context while connecting it to situation controllability.

STUDY 4

Study 4 aimed to further test our proposed mechanism through the mediating role of resource control within the broader theoretical model depicted in Figure 1. To enhance ecological validity, we created a user interface for a novel mobile app and asked participants to evaluate it and decide whether to adopt the app based on its features and privacy policy. This study therefore seeks to test consumers' control-reclaiming behavior through a routine decision to either keep a mobile app or switch to a competing app, while experimentally manipulating industry variability and violation type.

This study also aimed to rule out an alternative explanation. Martin, Borah, and Palmatier (2017) suggest that consumer vulnerability—perceived susceptibility to harm that arises from feelings of loss of control (Baker, Gentry, and Rittenburg 2005)—explains the impact of data breaches on consumer response. However, as conceptualized in the literature, consumer vulnerability arises primarily in extreme circumstances that present an imminent threat to safety.

In a majority of routine privacy situations, however, consumers are less likely to feel a sense of personal danger, instead sensing a more generalized loss of control over personal information (Draper and Turow 2019). Consistent with recent survey research (Pew 2019), our theorizing therefore suggests that resource control (and not vulnerability) is the primary driving force underlying consumer response to most routine privacy violations.

Method

Sample and design. Participants were 1,022 US residents recruited from MTurk and randomly assigned to conditions in a 2 (violation type: *targeting, sharing*) × 2 (industry variability: low, high) between-participants experiment. We oversampled to account for those with no interest in the mobile app category, aiming to retain at least 100 participants per condition. This is because consumers who lack interest in a product category are unlikely to be influenced by the type of privacy violation, regardless of situation controllability (Plangger and Montecchi 2020). Excluding these participants left a sample of N = 627 (N = 500 after attention check exclusions, $M_{Age} = 36.53$, $SD_{Age} = 11.98$; 50.40% female).

Stimuli and procedure. Participants were first told that they were to evaluate a location service app called CrowdChkr, which informed users how crowded public locations are. As part of the app demo process, participants were asked to provide their initials and zip code to simulate the type of personal information consumers would be asked to give to an actual mobile app. Participants were then asked to try a demo of the app's user interface. As shown in Appendix F, the interface featured a generic map with a few marked locations. Participants were reassured that this was only a demo and not linked to their actual location. When participants clicked on these different locations, details of the current occupancies of the respective places appeared. To

maintain the cover story, participants were then asked to evaluate their overall impression of the app's main features and provide qualitative feedback.

After completing the demo, participants were told that, using their provided information, a CrowdChkr account had been automatically created for them with a username piped from the initials and zip code input at the beginning of the study. As users of the CrowdChckr app, they were then presented with the app's privacy policy. In the *sharing* (*targeting*) condition, the privacy policy notified participants that the app collected information regarding users' contact details and location, and that this information would be shared with a third-party (used to deliver targeted ads). Participants were then provided with additional information as part of the industry variability manipulation (see Appendix F). In the high (low) variability condition, an animated GIF informed participants that there are many other location service apps in the industry, and that all of them have the same (a different) privacy policy with respect to users' data.

For the main dependent measure, participants were presented with three options. They could choose to keep their CrowdChkr account and receive an email with a link to download the app (0), they could delete their account and try another similar app (1), or they could delete the account and not try any other app (2). As described earlier, those who chose the latter option indicated no interest in the product category and were excluded from further analyses. A logistic regression confirmed that neither violation type nor industry variability influenced participants' selection of this "no interest" option (vs. others; all *p*s >.12, see Appendix G). The remaining options therefore created a dichotomous choice measure of brand switching. Consistent with our previous studies, participants also indicated how strongly they felt about their choice. The two measures (r = .95) were again standardized and averaged into a switching index. Resource control was also measured as a potential mediator, using a single item adapted from Ajzen

(2002): "How much control do you feel over your information on CrowdChkr?" (1 = *No control at all*, 9 = *A lot of control*). Additionally, to test consumer vulnerability as a potential alternative explanation, participants completed a three-item, nine-point measure of vulnerability (Martin, Borah, and Palmatier 2017). As a check on the industry variability manipulation, participants were then asked to rate the level of variability in privacy practice in the location service industry on a scale from 1 (*All have the same privacy policies*) to 9 (*All have the different privacy policies*). Finally, participants responded to an attention check concerning CrowdChkr's privacy policy and provided demographic information.

Results

Manipulation check. A 2 (violation type) × 2 (industry variability) factorial ANOVA on the variability check revealed that those in the high (low) variability condition perceived a significantly higher level of variability in privacy practice in the industry ($F(1, 496) = 210.14$, $p < .001$, $M_{\text{High Variability}} = 7.11$, $SD_{\text{High Variability}} = 1.64$, $M_{\text{Low Variability}} = 4.04$, $SD_{\text{Low Variability}} = 2.92$). There was no main effect of violation type or interaction effect (*p*s > .41), indicating that the manipulation was successful.

Main effects and interaction. We conducted a 2 (violation type) × 2 (industry variability) factorial ANOVA on resource control. As expected, results showed only a significant main effect of violation type on control ($F(1, 496) = 7.07$, $p < .01$; other *p*s > .33), such that *sharing* (M = 5.10, SD = 2.50) reduced feelings of control over personal information relative to *targeting* (M = 5.66, SD = 2.24). This lends further support to our theorizing that severity of privacy violation influences consumers' sense of resource control regardless of industry characteristics.

A parallel 2 (violation type) × 2 (industry variability) factorial ANOVA on the switching index revealed no main effect of violation type ($p = .47$) but a significant main effect of industry

variability ($F(1, 496) = 5.49$, $p = .02$) such that participants were less likely to switch under low ($M = -0.70$, $SD = 0.69$) versus high industry variability ($M = -0.55$, $SD = 0.83$). We again observed the expected two-way interaction on switching ($F(1, 496) = 4.49$, $p = .04$; Figure 5). Decomposing this interaction further supported our theorizing. When industry variability was high, *sharing* ($M = -0.44$, $SD = 0.87$) prompted a greater likelihood of switching as compared to *targeting* ($M= -0.64$, $SD = 0.77$, $p = .04$). In contrast, when industry variability was low, there was no significant difference in switching between *targeting* and *sharing* ($p = .33$).

Moderated mediation. Our theorizing (as summarized in Figure 1) suggests that severe (vs. moderate) privacy violations increase consumers' active coping behaviors because they reduce resource control. We have further argued and shown that this active coping response is attenuated when situation controllability (operationalized as industry variability) is low. If true, resource control should mediate the relationship between violation type and switching under high industry variability, but the mediated effect should be significantly attenuated under low industry variability. This was tested via moderated mediation analysis using the PROCESS Macro (Hayes 2013; Model 15) with violation type as the predictor, resource control the mediator, industry variability the moderator, and switching the dependent measure.

Results supported our theorizing. First, we observed the expected resource control × industry variability interaction on switching ($b = -0.08$, $SE = 0.03$, $p < .01$; see Appendix H for visualization of interaction). Planned contrasts revealed that, as predicted, resource control exhibited a strong negative relationship with switching behavior in the high variability condition ($b = -0.15$, $SE = 0.02$, $p < .001$) but an attenuated relationship in the low variability condition ($b = -0.06$, $SE = 0.22$, $p = .001$). Results also revealed a significant index of moderated mediation (index = 0.05, SE = 0.02, $CI_{.95}$ [0.01,0.10]; Figure 6), suggesting that the overall model was

significant. Specifically, when industry variability was high, *sharing* (vs. *targeting*) reduced feelings of resource control, which in turn increased participants' likelihood of switching (ab = 0.08, SE = 0.03, $CI_{.95}$ [0.02,0.15]). However, when industry variability was low, the indirect effect of violation type on switching through resource control was significantly attenuated (ab = 0.04, SE = 0.02, $CI_{.95}$ [0.005, 0.08]).

Finally, we ran additional analyses to test for consumer vulnerability as an alternative mechanism. Including vulnerability as a covariate in the moderated mediation model did not change the results. The index of moderated mediation was still significant (index = 0.04, SE = 0.02, $CI_{.95}$ [0.01, 0.09]), reflecting the same pattern of conditional effects as the model without vulnerability. Additionally, a separate moderated mediation analysis with both resource control and vulnerability as parallel mediators showed a significant index of moderated mediation with resource control as the mediator (index = 0.04, SE = 0.02, $CI_{.95}$ [0.01, 0.09]), but not with vulnerability as the mediator (index = 0.02, SE = 0.02, $CI_{.95}$ [-0.01, 0.07]). Thus, while vulnerability may explain consumer response to privacy violations in some contexts, our theorizing and findings suggest that resource control serves as a more robust mechanism.

Discussion

Study 4 findings further solidify our theorizing. When situation controllability (as industry variability) was high, *sharing* (vs. *targeting*) reduced feelings of control over consumers' own personal information, which in turn increased control-reclaiming behaviors (as brand switching). However, when situation controllability was low, violation type still affected resource control but these feelings of control were in turn less likely to translate into control-reclaiming behavior. Furthermore, our results rule out consumer vulnerability as an alternative mechanism, suggesting that consumers' seemingly paradoxical privacy behaviors are primarily

rooted in their need to regain lost control. This provides additional support for our theorizing around the roles of resource control and situation controllability in explaining the privacy paradox. In addition, we found no significant main effect of industry variability on perceived control, supporting our underlying assumption that situation controllability acts as enabler of control-reclaiming behaviors, not as a *source* of control. In our final study, we aimed to replicate the core violation type × industry variability interaction in an actual market setting and using an alternative form of control-reclaiming behavior.

STUDY 5

Study 5 used text analysis of Twitter data to compare linguistic response to *targeting* or *sharing* privacy violations from Facebook and Amazon, creating a naturalistic 2 (violation type: *targeting*, *sharing*) × 2 (company: Facebook, Amazon) quasi-experiment. Facebook and Amazon represent two industries (online retail and social media) that differ in terms of variability of privacy practices. We expect increased control-reclaiming behavior in response to a *sharing* (vs. *targeting*) privacy violation from Facebook because it operates in an industry with high variability in privacy practice (Ahmad 2018; Norton 2020). However, because Amazon operates in a more standardized industry (Paul 2020), a sense of helplessness should inhibit consumers' control-reclaiming behavior regardless of the company's privacy-violating action.

To operationalize control-reclaiming behavior, we draw from research in psycholinguistics on the use of personal pronouns. Personal pronouns have been shown to demonstrate a speaker's mental state or traits and influence cognitive processes (Chung and Pennebaker 2007; Kacewicz et al. 2014). In marketing and related fields, research into personal pronouns has grown in prominence in recent years thanks to the increasing availability of text

data. Research in this domain has shown that use of personal pronouns can affect relationships between firms and customers (Packard, Moore, and McFerran 2018) or influence cultural trends (Packard and Berger 2020). More relevant to the present study, Kacewicz et al. (2014) established that use of first-person plural ("we") and second-person singular ("you") pronouns both serve as verbal expressions of control because they imply a collectivist- and other-orientation, respectively (Cassell et al. 2006). Use of such control-enhancing language can serve as a way for individuals to reclaim control once it has been threatened, even if the individual is not consciously aware of it (Thimm, Rademacher, and Kruse 1995). We therefore expect greater frequency of these control-enhancing pronouns among consumers tweeting about Facebook's *sharing* (vs. *targeting*) privacy violations because situation controllability is relatively high. Conversely, in response to Amazon (where situation controllability is low), pronoun frequency should not differ regardless of whether the tweets refer to *sharing* or *targeting*.

Method

We used package Rtweet to collect 4,165 tweets (N = 3,805 after removing duplicates) from the Twitter Developer API and matched keywords (Hewett et al. 2016) reflecting violation type (*targeting* or *sharing*) with either Amazon or Facebook. Keywords regarding *targeting* (*sharing*) were "targeting," "targeted," "targets" ("sharing data," "shares data," "shared data," "third party data," "3rd party data"). Following Berger et al. (2020), we excluded retweets and replies to ensure that the content was not biased towards the most popular tweets, and removed URLs, punctuation, digits, username tags, and emojis (see Table 2 for example tweets). We ran the cleaned data through the LIWC Dictionary (Pennebaker et al. 2015) to analyze frequencies (per tweet) of two linguistic expressions of control enhancement: Pronouns "we" and "you."

Results

A 2 (violation type) × 2 (company) ANOVA (df = 1, 3801 for F-tests) treating "we" frequency as the dependent variable revealed no main effects (*p*s > .17), but a significant interaction (F = 6.85, $p = .009$). Planned contrasts supported our theorizing. For tweets referencing Facebook (Figure 7a), *sharing* (vs. *targeting*) was associated with significantly greater usage of "we" (F = 6.85, $p = .009$, $M_{Sharing} = 0.78$, $SD_{Sharing} = 2.53$, $M_{Targeting} = 0.41$, $SD_{Targeting} = 1.58$), whereas no effect of violation type was observed among tweets referencing Amazon ($p = .14$). A parallel ANOVA on "you" frequency displayed a similar pattern. Although we observed main effects of violation type (F = 96.15, $p < .001$) and company (F = 29.38, $p < .001$), this was qualified by a significant interaction (F = 70.49, $p < .001$, Figure 7b). Planned contrasts again showed, with reference to Facebook, usage of "you" was significantly greater in response to *sharing* (vs. *targeting*; F = 189.60, $p < .001$, $M_{Sharing} = 3.06$, $SD_{Sharing} = 4.60$, $M_{Targeting} = 0.74$, $SD_{Targeting} = 2.25$), whereas no difference emerged with reference to Amazon ($p = .54$, $M_{Sharing} = 0.74$, $SD_{Sharing} = 2.18$, $M_{Targeting} = 0.65$, $SD_{Targeting} = 2.14$).

Discussion

Consistent with our theorizing, consumers use control-signaling pronouns much more frequently when they discuss Facebook's *sharing* (vs. *targeting*) actions. The same effect, however, is not observed when discussing Amazon, even though its actions are no less intrusive than Facebook's. This is because Facebook and Amazon, while equally intrusive with consumers' data, operate in industries with highly different privacy norms.

One potential alternative explanation for this pattern is that the pronoun "you" was more popular with Facebook due to the highly social aspect of the platform. Indeed, Packard and Berger (2020) found that songs with "you" are much more popular because "you" directly

signals attentional focus and inspires other-activation. Yet the authors did not find the same effect on usage of "we." In contrast, this quasi-experiment found converging findings on both "we" and "you" and therefore, in conjunction with our prior studies, provides robust support for our theorizing around consumers' usage of these pronouns as a means to reclaim control.

GENERAL DISCUSSION

The rapid development of big data analytics (e.g., machine learning, deep learning, artificial intelligence, etc.) suggests that collection and use of consumers' personal data will only continue to grow. Privacy is therefore more prescient to marketers and consumers than ever before (Martin, Borah, and Palmatier 2017). Yet, the literature provides little clarity around the construct of privacy violation (Martin and Murphy 2017) and the privacy paradox (Krasnova et al. 2010). The current research aimed to contribute to these overlapping areas.

Inspired by in-depth interviews with privacy experts, Study 1 revealed three dimensions of privacy violation (*recording*, *targeting*, and *sharing*) that progressively increase in severity. Four subsequent studies then converged to show that severe (vs. moderate) privacy violations progressively diminish consumers' perceived control over a valued resource (i.e., resource control), prompting a greater likelihood of control-reclaiming behaviors. Consistent with this mechanism, our research also demonstrates the moderating role of situation controllability (as industry variability) that helps explain the privacy paradox. Study 2 confirmed the effect of violation type on consumers' response using a direct manipulation of industry variability. Study 3 employed a lab experiment and showed that an incidental source of resource control may serve to attenuate the effects of violation type, further supporting resource control as the mechanism. Study 4 then provided mediation evidence for the proposed mechanism in an ecologically valid

setting with a consequential outcome. Lastly, Study 5 reinforced this pattern of effects using text analysis of Twitter data in a naturalistic, quasi-experimental design.

Theoretical Implications

The current research contributes to theories of consumer privacy by clarifying the construct of privacy violation from a consumer perspective. Because perceived privacy violation is a consumer-level construct, it is crucial to theory development that the construct be examined from the perspective of consumers, rather than academics or practitioners (Reich and Yuan 2019). Indeed, our studies show that consumers may understand privacy violations in a unique way depending on whether the company is *recording*, *targeting* or *sharing* consumer data. Importantly, building on existing conceptualizations, we show that perceptions of privacy violation hinge primarily on what companies do with consumers' information, rather than merely the nature or quantity of information collected. For instance, contrary to predominant definitions of privacy violation in the marketing literature (Nill and Aalberts 2014), our research suggests that consumers might not see merely being tracked or recorded online as particularly intrusive. Further, consumers might not perceive a highly targeted ad as especially violating, at least relative to having their data shared with third parties. In this aspect, we also disentangle the nuanced difference between *targeting* and *sharing*, two violation types traditionally confounded in past literature (Vesanen and Raulas 2006). Importantly, our research establishes that more severe violation types increase consumers' likelihood of engaging in control-reclaiming behaviors because violation severity reduces resource control.

Relatedly, our research establishes the underlying role of control in consumers' response to privacy behaviors as both a manipulated moderator (Study 3) and a measured mediator (Study 4). In so doing, this research extends beyond surface-level consequences (e.g., privacy concerns,

perceived risks, etc.; Brandimarte, Acquisti, and Loewenstein 2012; Krasnova et al. 2010; Phelps, Nowak, and Ferrell 2000) to contribute toward a deeper understanding of privacy from a consumer psychology perspective (Krishna 2020). This is especially important in light of the privacy paradox, whereby privacy concerns often do not translate into corresponding behavioral responses (Norberg, Horne, and Horne 2007). Indeed, greater privacy concerns have been shown to *increase* consumers' voluntary information disclosure (Sheehan and Hoy 1999). Moreover, other researchers have lamented that self-reported privacy concerns fail to predict meaningful consumer outcomes (Bornschein, Schmidt, and Maier 2020; Martin, Borah, and Palmatier 2017) and have called for investigations into mechanisms that better explain consumer privacy behaviors. Our research answers these calls, demonstrating that consumer reactions to privacy violation are primarily rooted in a need to reclaim lost control over personal information.

In addition, the current research sheds light on an otherwise opaque privacy paradox documented in the literature (Acquisti, Brandimarte, and Loewenstein 2020; Krasnova et al. 2010; Li et al. 2017; Norberg, Horne, and Horne 2007) by synthesizing theories of self-determination (Deci and Ryan 2000) and coping (Dweck 2000). Because people cope passively with threats to control when situation controllability is low (Skinner and Zimmer-Gembeck 2011), privacy violations fail to prompt an active consumer response when market conditions make reclaiming control seem impossible. Just as consumers deleted Facebook but continued with Amazon following similar privacy violations, our findings show that consumers are more likely to attempt to reclaim control (through brand switching [Studies 2-4] or status-enhancing language [Study 5]) only in an industry with high of variability in privacy practices. In contrast, in an industry in which most or all companies are using consumer data in the same way (i.e., when industry variability is low), consumers will be less likely to reclaim control regardless of

violation severity. This provides a robust theory-driven explanation for the privacy paradox that can be seen when comparing consumer behavior in industries with a relatively standardized data protection policy (e.g., online retail, banking, search engines, etc.; Grosso et al. 2020; Norberg, Horne, and Horne 2007) to those with high variability of privacy practices (e.g., social media, streaming, gaming, etc.; Hajli and Lin 2016). In so doing, the current research extends a privacy literature that has previously relied more narrowly on individual differences to explain consumer response to privacy violations (Aguirre et al. 2014; Hallam and Zanella 2017; Norberg, Horne, and Horne 2007).

Managerial Implications

As consumer data become more valuable to companies' business models (Interactive Advertising Bureau 2019), marketers must understand how consumers evaluate their data practice and strive to maintain a healthy balance between providing customized experiences and preserving consumer privacy. Our research shows that not all privacy violations are equal and violation severity has meaningful consequences for brands. Specifically, companies are more likely to alienate consumers as their violating actions shift from *recording* to *targeting* and to *sharing*, especially when asking for broad consent of personal information in vague terms. Yet certain information (e.g., crash reports) is important for companies to collect to improve consumer experience (Acquisti, Taylor, and Wagman 2016). As our findings suggest, a more balanced approach may be optimal, where companies ask consumers for consent to each data practice separately. For example, a mobile phone company could ask, separately, for consent to (1) record information regarding phone performance and errors, (2) use personal information to deliver targeted offerings, and (3) share certain information with a third party. Such a practice

could encourage consumers to continue to engage with the company and share their information as appropriate while preserving consumers' sense of control over their personal information.

In addition, past research has shown that while privacy is important to business practice, it is often seen as a burden or cost and could hardly be used strategically (Bamberger and Mulligan 2010; Martin and Murphy 2017). However, our findings suggest that privacy could be used as a unique selling point for a newcomer or a disadvantaged competitor in industries with standardized privacy practices. Indeed, DuckDuckGo—a private search engine platform—has gained substantial attention for its consumer-friendly privacy practices amid the otherwise Google-dominated search engine sphere (Lomas 2019). In addition, iPhone's newest advertising campaign has embraced privacy to differentiate themselves in an increasingly Android-dominated market (Grothaus 2020). In sum, it appears that standardized industries offer profound differentiation opportunities for marketers that may simultaneously enhance profitability and consumer well-being.

Finally, in establishing the moderating effect of situation controllability (as industry variability in data practice), our research suggests that consumers are especially susceptible to severe privacy violations in industries with standardized privacy practices (e.g., banking or online retail). Consequently, these industries require more attention and regulation from policy-makers. As an example of a feasible regulatory action, policy-makers might consider prohibiting privacy policy standardization by mandating a certain level of industry variability, thereby enhancing situation controllability by permitting consumer choice.

Limitations and Future Research

Although we have attempted to maximize the rigor of our research, several limitations exist that provide opportunities for future research. First, although Study 4 adopted a realistic

consumption setting and Study 5 employed naturalistic observation of online behavior, none of our studies employed a true field-experiment design in which random assignment of conditions was linked to actual marketplace behavior. One possible approach to doing so would be to deliver manipulated cookies policy pop-ups (similar to Studies 2 and 3) during consumer visits to actual company websites, and observing naturalistic responses without their awareness that they are participating in a research study. Although such an endeavor requires ambitious effort, it would be a worthwhile extension of the current research.

In addition, although we have established industry variability as an explanatory factor for the privacy paradox, other factors may contribute to the phenomenon as well. For instance, brand loyalty has been shown to increase consumers' willingness to forgive a company for unethical behavior (Ingram, Skinner, and Taylor 2005) and service failure (Henderson, Beck, and Palmatier 2011). It may therefore also serve as a consumer- and brand-level factor that helps explain why consumers sometimes fail to act on their privacy concerns. In an effort to develop a broader model of consumer privacy behavior, future researchers may explore this and other moderating factors at multiple levels (consumer, company, industry, etc.).

Moreover, our findings are subject to cultural variations in privacy norms. Research has shown that levels of privacy tolerance differ widely across cultures (Markos, Milne, and Peltier 2017). A more collectivist society might be more accepting towards data *sharing* whereas a more individualistic society might react more negatively to the control threat posed by these privacy violations. Future work should investigate these and other issues related to the generalizablity of our findings across cultural contexts.

Finally, across studies, we demonstrate consumers' coping response to a loss of resource control. However, compensatory control theory focuses on *personal* control—one's belief in

their ability to achieve desired outcomes (Landau, Kay, and Whitson 2015)—as a determinant of coping strategies. An outstanding question is, therefore, what is the link between resource control and personal control? Although one might assume that both types of control are always positively associated, situations in which relinquishing control over information (thereby reducing resource control) is necessary to gain access to an app that could help them achieve certain outcomes (thereby enhancing personal control). This interplay between resource control and personal control represents an interesting and important venue for future research, especially in the consumer privacy domain.

APPENDIX

Appendix A: Results of Study 1 Replication with Student Sample

Scenario	Description	Perceived privacy violation (Mean)	SD	Comp1 3.70*	Comp2 1.51*	Comp3 1.19*	Factor
Discount Scan	A retailer offers discounts to its members when they scan their mobile barcode from the membership app.	2.22	1.47	0.66			Recording
CashierZip	A cashier asks for a customer's zip code at check out	2.79	1.73	0.59			
CCTV	CCTV in the supermarket aisle that tracks customers' activity in-store.	3.71	1.92	0.70			
Coupon Phone	A supermarket app provides coupons of produce on a customer's phone when s/he around the produce section in-store.	3.77	1.89	0.77			
DNAsite	DNA information submitted to an online genealogy website is used to identify a suspect in a criminal case.	4.61	1.75		0.30		Targeting
Search History	A company uses search history to provide ads that are specifically tailored to users.	4.59	2.10		0.61		
SMTarget Ads	A social media app uses users' shared information to provide targeted advertising under sponsored posts.	4.67	1.72		0.75		
Home-Sharing	A home sharing app uses users' search history to predict high-demand dates and set prices accordingly.	4.84	1.77		0.44		
Pregnancy Ads	A retailer uses a customer's purchase history to predict that a customer is pregnant and send pregnancy advertisements to her address.	5.22	1.88		0.78		
Mobile Service	A mobile network provider offers a service to other companies to use the provider's customer call & browsing info to map locations & apps usage	5.89	1.34			0.71	Sharing
Developer Access	A social media app allows third-party developers access to users' data.	6.06	1.34			0.68	
Record Convo	A smart home device accidentally records and sends a conversation of a user to another person.	6.52	1.09			0.62	

Notes: *component Eigenvalue; numbers within bars represent means; error bars represent 95% CI; numbers in component columns represent factor loadings.

113 students (N = 113; M_{Age} = 25.85, SD_{Age} = 7.32; 67.0% female) at a public university participated in this replication study in exchange for course credit. A Principal Component Analysis (PCA) with Varimax rotation found that the twelve ratings converged into three components with step levels of perceived privacy violation. A follow-up repeated-measures ANOVA comparing the composite means of these components suggested a significant omnibus difference (Hyunh-Feldt $F(2, 224) = 293.80$, $p < .001$, replicating results of the main study.

Appendix B. Violation type Manipulation (Study 2 and 3)

Recording Condition

Imagine that you are shopping online/ browsing social media. You have bought products from this online retailer/have used this social media in the past and are returning today. As you are browsing, and a small pop-up window appears:

COOKIES POLICY

We use cookies to make sure that you have the best experience on our website. We'll collect and record your information on the websites you visit, the duration of visits, and your IP address.

This information will be used to improve your browsing experience, but will **NOT** be used to deliver customized advertisements and will **NOT** be shared with any third-party companies and developers.

You recently learned that this cookies practice helps the company earn an annual amount of $10 per user.

Targeting condition

COOKIES POLICY

We use cookies to make sure that you have the best experience on our website. We'll collect and record your information on the websites you visit, the duration of visits, and your IP address.

This information will be used to improve your browsing experience and deliver customized advertisements but will **NOT** be shared with any third-party companies and developers.

Sharing condition

COOKIES POLICY

We use cookies to make sure that you have the best experience on our website. We'll collect and record your information on the websites you visit, the duration of visits, and your IP address.

This information will be used to improve your browsing experience and share with several registered third party companies but will **NOT** be used for targeted advertisements.

Appendix C: Measures used across Studies

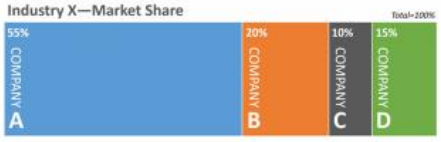
Measure	Item	Study
Privacy violation	• "This action is…" (1 = Not at all a privacy violation; 7 = An extreme privacy violation).	1
Privacy violation (Krasnova et al. 2010)	• "This action is…" (1 = *Not at all a privacy violation*; 7 = *An extreme privacy violation*). • "Overall I see no real threat to my privacy due to my participation in this website" (1 = *Strongly disagree*; 7= *Strongly Agree*) • "I feel my personal information is safe on this website" (1 = *Strongly disagree*; 7= *Strongly Agree*) • Overall perception of privacy risk involved when using Company A's website (1 = *Not risky at all*; 7 = *Very risky*)	2 (pretest)
Brand Switching Index	• In this situation, would you continue on to Company A's website, or would you switch to another company's website to meet your needs? I would… (0 = *Continue with Company A*, 1 = *Switch to another company*) • How strongly do you feel about your choice? (1 = *I feel strongly about continuing with company A*, 13 = *I feel strongly about switching to another company*)	2, 3
Brand Switching Index	• In this situation, would you continue on to Company A's website, or would you switch to another company's website to meet your needs? I would… (0 = *Keep my account on CrowdChkr and receive an email with the download link*, 1 = *Delete my account on CrowdChkr and switch to another similar app*, 2 = *Delete my account on CrowdChkr and do not try another similar app*) • How strongly do you feel about your choice? (1 = *I feel strongly about keeping my CrowdChkr account*, 13 = *I feel strongly about switching to another similar app*)	4
Resource Control (Ajzen 2002)	• I feel in control over this process (1= *Strongly disagree*; 5= *Strongly agree*) • It is easy for me to complete this process (1= *Strongly disagree*; 5= *Strongly agree*)	3
Resource Control (Ajzen 2002)	• How much control do you feel over your information on CrowdChkr? (1 = *No control at all over my information*; 9 = *Complete control over my information*)	4

Vulnerability (Martin, Borah, and Palmatier 2017)	• How do the personal data practices in this situation make you feel:
	  ○ vulnerable (1 = *Not at all vulnerable*; 9 = E*xtremely vulnerable*)
	  ○ exposed (1 = *Not at all exposed*; 9 = *Extremely exposed*)
	  ○ threated (1 = *Not at all threatened*; 9 = *Extremely threatened*)
		4

Variability Check	• How much variety is there in privacy policies of companies in Industry X? (1 = *All have the same privacy policies*; 7 = *All have different privacy policies*)	2, 5
Benefit Check	• This data practice primarily benefits…. (1 = *Company A*, 7 = *Consumers*)	2

Appendix D: Variability Manipulation, Study 2

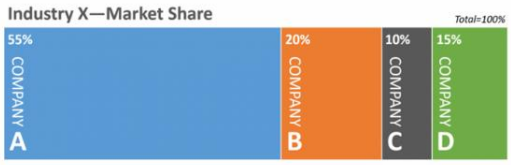
Industry X is comprised of many companies. The four largest companies in Industry X are labeled A, B, C, and D. The image below shows the relative market share (in %) of each of these four companies. That is, Company A has the largest share of the market (55%) in Industry X, Company B has the second largest share (20%), etc.



In addition, every company in Industry X requests the same personal information from consumers when they create their online account on the company's website.

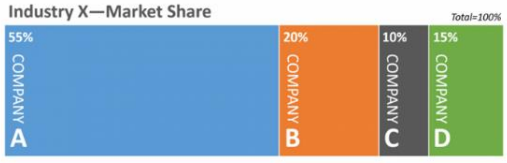
Low variability

Consumer information policy: Each company in Industry X uses consumers' personal information **in the same way** because Industry X **has a standard policy** regarding usage of personal consumer information.



High variability

Consumer information policy: Each company in Industry X uses consumers' personal information **in a different way** because Industry X **doesn't have a standard policy** regarding usage of personal consumer information.

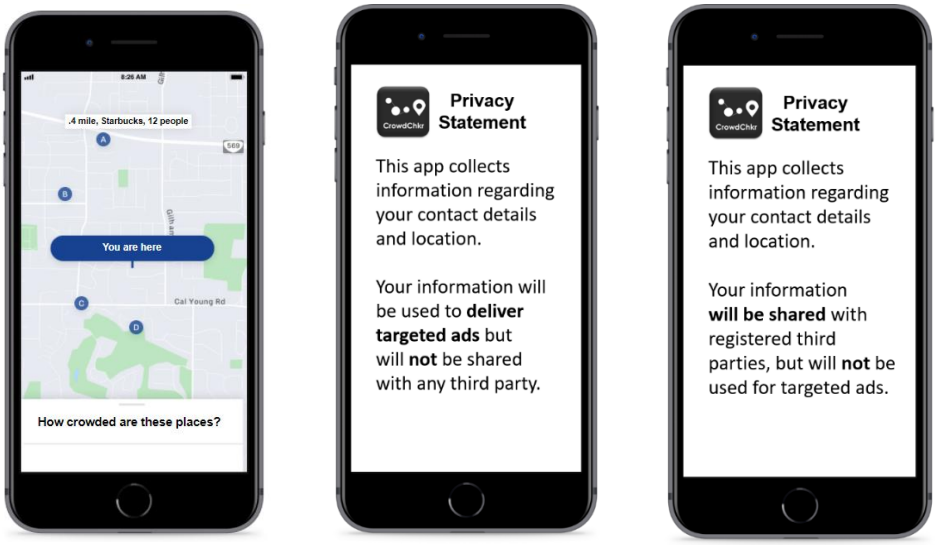


Appendix E: Main Effects and Interactions on Individual Switching Items and Combined Switching Index (Studies 2 – 4)

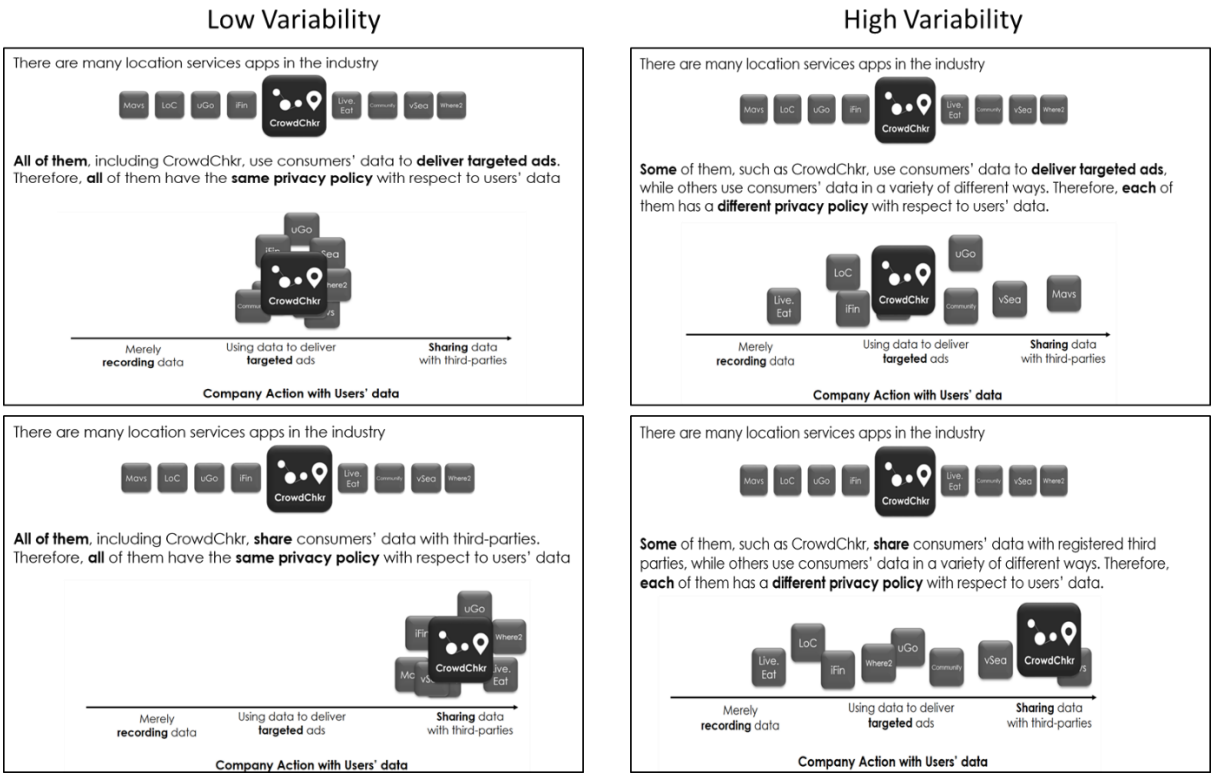
	Dichotomous switching item (Logistic Regression – Likelihood ratio test)			**Continuous switching item (ANOVA)**			**Combined switching index (ANOVA)**		
	df	χ^2	*p*	df	F	*p*	df	F	*p*
Study 2									
Violation Type	2	32.87	<.001	2,379	20.74	<.001	2,379	20.51	<.001
Industry Variability	1	17.39	<.001	1,379	13.05	<.001	1,379	13.23	<.001
Violation Type × Industry Variability	2	5.46	.06	2,379	8.05	<.001	2,379	7.42	<.001
Study 3									
Violation Type	1	10.67	.001	1,183	8.82	.003	1,183	10.77	.001
Resource Control	1	0.01	.91	1,183	0.79	.38	1,183	0.57	.45
Violation Type × Resource Control	1	4.30	.04	1,183	3.48	.06	1,183	4.35	.04
Study 4									
Violation Type	1	0.61	.43	1,496	0.42	.51	1,496	0.54	.47
Industry Variability	1	5.29	.02	1,496	4.98	.03	1,496	5.49	.02
Violation Type × Industry Variability	1	3.69	.05	1,496	4.68	.03	1,496	4.49	.04

Appendix F: Stimuli for Study 4

App Interface & Violation Types Manipulation



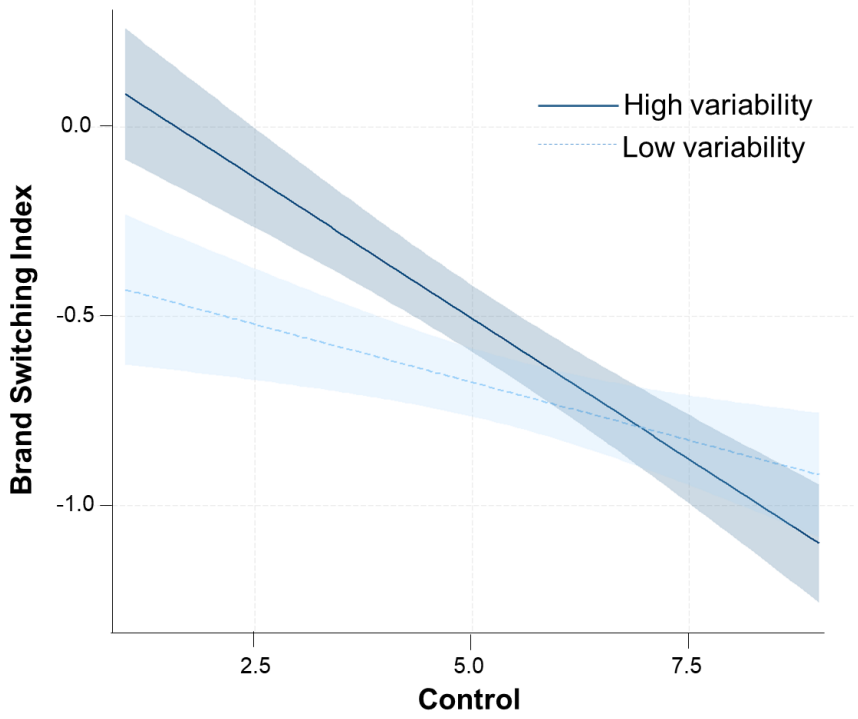
Variability Manipulation



Appendix G: Results of Logistic Regression on No-Interest Choice (Study 4)

In Study 4, to test whether participants who had no interest in the mobile app were equally distributed among experimental conditions, we dummy-coded a no-interest variable (1= *Delete and don't try any other app*, 0 = *Other choices*). We then conducted a logistic regression of violation type, industry variability, and their interaction on the no-interest measure and found no significant effects (*p*s > .12). This confirmed our assumption that participants who lack interest in a product category are unlikely to be influenced by the type of privacy violation or industry variability.

Appendix H: Resource Control × Industry Variability on Brand Switching (Study 4)



REFERENCES

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2020), "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age," *Journal of Consumer Psychology*, 30 (4), 736–58.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman (2016), "The Economics of Privacy," *Journal of Economic Literature*, 54 (2), 442–92.

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter, and Martin Wetzels (2014), "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing*, 91 (1), 34–49.

Ahmad, Irfan (2018), "How do Social Platforms Protect Your Information? [Infographic] | Social Media Today," *Social Media Today*.

Ajzen, Icek (2002), "Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior," *Journal of Applied Social Psychology*, 32 (4), 665–83.

Awad, Naveen Farag and Mayuram S Krishnan (2006), "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly*, 30 (1), 13–28.

Baker, Stacey Menzel, James W Gentry, and Terri L Rittenburg (2005), "Building Understanding of the Domain of Consumer Vulnerability," *Journal of Macromarketing*, 25 (2), 128–39.

Bamberger, Kenneth A and Deirdre K Mulligan (2010), "Privacy on the Books and on the Ground," *Stanford Law Review*, 63, 247–316.

Baumeister, Roy F, Liqing Zhang, and Kathleen D Vohs (2004), "Gossip as Cultural Learning," *Review of General Psychology*, 8 (2), 111–21.

Benes, Ross (2018), "People Believe Ads Are Becoming More Intrusive," *eMarketer*.

Bornschein, Rico, Lennard Schmidt, and Erik Maier (2020), "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices," *Journal of Public Policy & Marketing*, 39 (2), 135–54.

Brandeis, Samuel D and Louis D Warren (1890), "The Right to Privacy," *Harvard Law Review*, 4 (5), 193–220.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein (2012), "Misplaced Confidences," *Social Psychological and Personality Science*, 4 (3), 340–47.

Chung, Cindy and James W Pennebaker (2007), "The Psychological Functions of Function words," *Social Communication*, 1, 343–59.

Chung, Tuck Siong, Michel Wedel, and Roland T Rust (2016), "Adaptive Personalization Using Social Networks," *Journal of the Academy of Marketing Science*, 44 (1), 66–87.

Deci, Edward L and Richard M Ryan (2000), "The" What" and" Why" of Goal Pursuits: Human Needs and the Self-determination of ehavior," *Psychological inquiry*, 11 (4), 227–68.

Draper, Nora A and Joseph Turow (2019), "The Corporate Cultivation of Digital Resignation," *New Media & Society*, 21 (8), 1824–39.

Dweck, Carol S (2000), *Self-theories: Their Role in Motivation, Personality, and Development*, United Kingdom: Psychology Press.

Fast, Nathanael J, Deborah H Gruenfeld, Niro Sivanathan, and Adam D Galinsky (2009), "Illusory Control: A Generative Force behind Power's Far-reaching Effects," *Psychological Science*, 20 (4), 502–8.

Foster, Eric K (2004), "Research on Gossip: Taxonomy, Methods, and Future Directions,"

Review of General Psychology, 8 (2), 78–99.

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing*, 10 (1), 149–66.

Grosso, Monica, Sandro Castaldo, Hua Ariel Li, and Bart Larivière (2020), "What Information Do Shoppers Share? The Effect of Personnel-, Retailer-, and Country-Trust on Willingness to Share Information," *Journal of Retailing*, 96 (4), 524–47.

Grothaus, Michael (2020), "Apple's New Privacy Ad has a ton of Easter Eggs. Here's What They Refer to," *FastCompany*.

Hajli, Nick and Xiaolin Lin (2016), "Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information," *Journal of Business Ethics*, 133 (1), 111–23.

Hallam, Cory and Gianluca Zanella (2017), "Online Self-disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance between Concerns and Rewards," *Computers in Human Behavior*, 68, 217–27.

Harrell, Margaret C and Melissa A Bradley (2009), "Data Collection Methods. Semi-Structured Interviews and Focus Groups," Santa Monica, CA: Rand National Defense Research Institute.

Hayes, Andrew F (2013), *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-based Approach*, New York, NY, US: Guilford Press.

Henderson, Conor M, Joshua T Beck, and Robert W Palmatier (2011), "Review of the Theoretical Underpinnings of Loyalty Programs," *Journal of Consumer Psychology*, 21 (3), 256–76.

Hewett, Kelly, William Rand, Roland T Rust, and Harald J Van Heerde (2016), "Brand buzz in the echoverse," *Journal of Marketing*, 80 (3), 1–24.

Ingram, Rhea, Steven J Skinner, and Valerie A Taylor (2005), "Consumers' Evaluation of Unethical Marketing Behaviors: The Role of Customer Commitment," *Journal of Business Ethics*, 62 (3), 237–52.

Interactive Advertising Bureau (2019), "Digital Advertising Revenues Rise To $26.2 Billion In Q3 2018, Up 22% Year-Over-Year, According To IAB," *IAB*, New York, NY, US.

Irvine, Annie, Paul Drew, and Roy Sainsbury (2013), "'Am I not Answering Your Questions Properly?'Clarification, Adequacy and Responsiveness in Semi-structured Telephone and Face-to-face Interviews," *Qualitative Research*, 13 (1), 87–106.

Kacewicz, Ewa, James W Pennebaker, Matthew Davis, Moongee Jeon, and Arthur C Graesser (2014), "Pronoun Use Reflects Standings in Social Hierarchies," *Journal of Language and Social Psychology*, 33 (2), 125–43.

Kazienko, Przemysław and Michał Adamski (2007), "AdROSA—Adaptive Personalization of Web Advertising," *Information Sciences*, 177 (11), 2269–95.

Kirkpatrick, Marshall (2010), "Facebook's Zuckerberg Says The Age of Privacy Is Over," *The New York Times*.

Krasnova, Hanna, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand (2010), "Online Social Networks: Why We Disclose," *Journal of Information Technology*, 25 (2), 109–25.

Krishna, Aradhna (2020), "Privacy is a Concern: An Introduction to the Dialogue on Privacy," *Journal of Consumer Psychology*, 30 (4), 733–35.

Kurland, Nancy B and Lisa Hope Pelled (2000), "Passing the Word: Toward a Model of Gossip and Power in the Workplace," *Academy of Management Review*, 25 (2), 428–38.

Landau, Mark J, Aaron C Kay, and Jennifer A Whitson (2015), "Compensatory Control and the Appeal of a Structured World," *Psychological Bulletin*, 141 (3), 694.

Li, Han, Xin (Robert) Luo, Jie Zhang, and Heng Xu (2017), "Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors," *Information and Management*, 54 (8), 1012–22.

Lomas, Natasha (2019), "Google has Quietly Added DuckDuckGo as a Search Engine Option for Chrome Users in ~60 Markets," *Tech Crunch*.

Lynskey, Dorian (2019), "'Alexa, Are You Invading My Privacy?' – The Dark Side of Our Voice Assistants," *The Guardian*.

MacInnis, Deborah J, Vicki G Morwitz, Simona Botti, Donna L Hoffman, Robert V Kozinets, Donald R Lehmann, John G Lynch Jr, and Cornelia Pechmann (2020), "Creating Boundary-Breaking, Marketing-Relevant Consumer Research," *Journal of Marketing*, 84 (2), 1–23.

MacMillan, Douglas and Robert McMillan (2018), "Google Exposed User Data, Feared Repercussions of Disclosing to Public," *Wall Street Journal*.

Markos, Ereni, George R Milne, and James W Peltier (2017), "Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of The United States And Brazil," *Journal of Public Policy & Marketing*, 36 (1), 79–96.

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, Kelly D and Patrick E Murphy (2017), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science*, 45 (2), 135–55.

McAlister, Leigh, Max H Bazerman, and Peter Fader (1986), "Power and Goal Setting in Channel Negotiations," *Journal of Marketing Research*, 23 (3), 228–36.

Mulligan, Deirdre K., Colin Koopman, and Nick Doty (2016), "Privacy is an Essentially Contested Concept: A Multi-dimensional Analytic for Mapping Privacy," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*,

374 (2083).

Nill, Alexander and Robert J. Aalberts (2014), "Legal and Ethical Challenges of Online Behavioral Targeting in Advertising," *Journal of Current Issues and Research in Advertising*, 35 (2), 126–46.

Nivea, Richard (2019), "At F8, Zuckerberg Unveils Facebook's New Mantra: 'The Future Is Private,'" *CNET*.

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.

Norton (2020), "Protecting your social media privacy | Norton," *Norton*.

Packard, Grant and Jonah Berger (2020), "Thinking of You: How Second-Person Pronouns Shape Cultural Success," *Psychological Science*, 31 (4), 397–407.

Packard, Grant, Sarah G Moore, and Brent McFerran (2018), "(I'm) Happy to Help (You): The Impact of Personal Pronoun Use in Customer–Firm Interactions," *Journal of Marketing Research*, 55 (4), 541–55.

Paul, Kari (2020), "They Know Us Better Than We Know Ourselves': How Amazon Tracked My Last Two Years of Reading," *The Guardian*.

Pew (2019), "Americans and Privacy: Concerned, Confused and Feeling Lack Of Control over Their Personal Information," *Pew Research Center*, Washington, DC.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell (2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, 19 (1), 27–41.

Plangger, Kirk and Matteo Montecchi (2020), "Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance," *Journal of Interactive Marketing*, 50, 32–44.

PWC (2017), "Consumer Intelligence Series: Protect Me," (September), 4.

Reich, Brandon J and Hong Yuan (2019), "A Shared Understanding: Redefining 'Sharing' from a Consumer Perspective," *Journal of Marketing Theory and Practice,* 27 (4), 430–44.

Rucker, Derek D, Adam D Galinsky, and David Dubois (2012), "Power and Consumer Behavior: How Power Shapes Who and What Consumers Value," *Journal of Consumer Psychology*, 22 (3), 352–68.

Schiele, Kristen and Alladi Venkatesh (2016), "Regaining Control through Reclamation: How Consumption Subcultures Preserve Meaning and Group Identity after Commodification," *Consumption Markets & Culture,* 19 (5), 427–50.

Sedek, Grzegorz, Miroslaw Kofta, and Tadeusz Tyszka (1993), "Effects of Uncontrollability on Subsequent Decision Making: Testing the Cognitive Exhaustion Hypothesis," *Journal of Personality and Social Psychology,* 65 (6), 1270–81.

Shane, Dakota (2018), "Research Shows Users Are Leaving Facebook in Droves. Here's What It Means For You," *INC.com*.

Sheehan, Kim Bartel (2002), "Toward a typology of Internet users and online privacy concerns," *The Information Society,* 18 (1), 21–32.

Sheehan, Kim Bartel and Mariea Grubbs Hoy (1999), "Using E-mail to Survey Internet Users in the United States: Methodology and Assessment," *Journal of Computer-Mediated Communication*, 4 (3), JCMC435.

Skinner, Ellen A (1996), "A Guide to Constructs of Control," *Journal of Personality and Social Psychology*, 71 (3), 549–70.

Skinner, Ellen A and Melanie J Zimmer-Gembeck (2011), "Perceived Control and the Development of Coping," in *The Oxford Handbook of Stress, Health, and Coping*, S. Folkman, ed., Oxford University Press, 35–59.

Smith, H Jeff, Tamara Dinev, and Heng Xu (2011), "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, 35 (4), 989–1015.

Summers, Christopher A, Robert W Smith, and Rebecca Walker Reczek (2016), "An Audience of One: Behaviorally Targeted Ads as Implied Social Labels," *Journal of Consumer Research*, 43 (1), 156–78.

Taylor, Charles R, George R Franke, and Michael L Maynard (2000), "Attitudes toward Direct Marketing and Its Regulation: A Comparison of The United States and Japan," *Journal of Public Policy & Marketing*, 19 (2), 228–37.

Thimm, Caja, Ute Rademacher, and Lenelis Kruse (1995), "' Power-Related Talk' Control in Verbal Interaction," *Journal of Language and Social Psychology*, 14 (4), 382–407.

Tucker, Catherine E. (2014), "Social Networks, Personalized Advertising, and Privacy Controls," *Journal of Marketing Research*, 51 (5), 546–62.

Vesanen, Jari and Mika Raulas (2006), "Building Bridges for Personalization: A Process Model for Marketing," *Journal of Interactive Marketing*, 20 (1), 5–20.

Wert, Sarah R and Peter Salovey (2004), "A Social Comparison Account of Gossip," *Review of General Psychology*, 8 (2), 122–37.

Whitson, Jennifer A and Adam D Galinsky (2008), "Lacking Control Increases Illusory Pattern Perception," *Science*, 322 (5898), 115–17.

Wuerthele, Mike (2019), "'Privacy. That's iPhone' ad Campaign Launches, Highlights Apple's Stance on User Protection," *AppleInsider*.

TABLE

Table 1. Study 1: PCA Results Ordered by Mean Score

Scenario	Description	Perceived privacy violation	Comp1 3.70*	Comp2 2.04*	Comp3 1.07*	Factor
Discount Scan	A retailer offers discounts to its members when they scan their mobile barcode from the membership app.	2.55	0.705			Recording
CashierZip	A cashier asks for a customer's zip code at check out	3.19	0.711			
Coupon Phone	A supermarket app provides coupons of produce on a customer's phone when s/he around the produce section in-store.	3.78	0.756			
CCTV	CCTV in the supermarket aisle that tracks customers' activity in-store.	4.01	0.651			
Search History	A company uses search history to provide ads that are specifically tailored to users.	4.89		0.768		Targeting
DNAsite	DNA information submitted to an online genealogy website is used to identify a suspect in a criminal case.	4.91		0.606		
SMTarget Ads	A social media app uses users' shared information to provide targeted advertising under sponsored posts.	5.12		0.777		
Home-Sharing	A home sharing app uses users' search history to predict high-demand dates and set prices accordingly.	5.14		0.743		
Pregnancy Ads	A retailer uses a customer's purchase history to predict that a customer is pregnant and send pregnancy advertisements to her address.	5.49		0.704		
Mobile Service	A mobile network provider offers a service to other companies to use the provider's customer call & browsing info to map locations & apps usage	6.04			0.764	Sharing
Developer Access	A social media app allows third-party developers access to users' data.	6.09			0.611	
Record Convo	A smart home device accidentally records and sends a conversation of a user to another person.	6.24			0.842	

Notes: *component Eigenvalue; numbers within bars represent means; error bars represent 95% CI; numbers in component columns represent factor loadings.

Table 2. Study 2: Examples of tweets collected in Study 5

	Amazon	Facebook
Targeting	"Targeted marketing tech allows the food industry to tailor promotions, transforming a one-time temptation into an all-the-time ad. 2/3 of products we purchased from @amazon were healthy, but the majority of ads after were for unhealthy food" (n= 299)	"Facebook refuses to restrict untruthful political ads and micro-targeting. You know what to do." (n=3171)
Sharing	Amazon has fired a number of employees after they shared customer email address and phone numbers with a third-party. Are you building your brand on Amazon? How do you control the security of your customers' private #data on that platform? (n=134)	"Facebook is normalizing sharing your healthcare data #privacy" (n=201)

FIGURE

Figure 1. Conceptual Framework of Constructs (bold) and Operationalizations (italics)

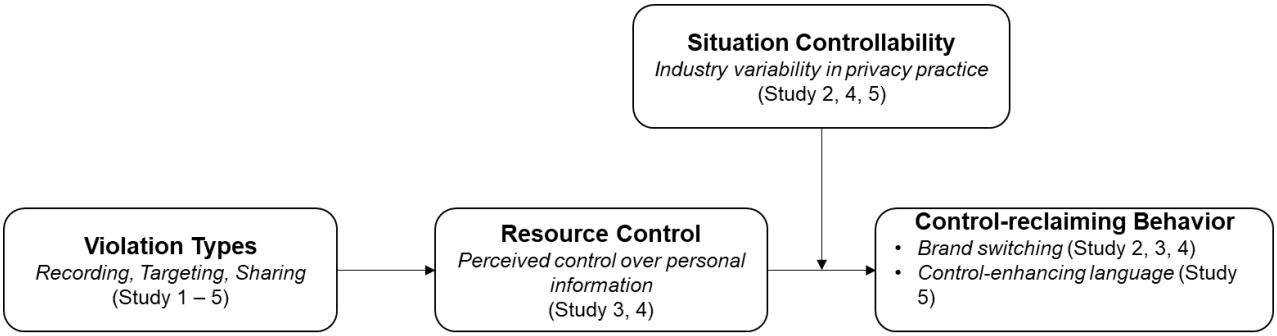
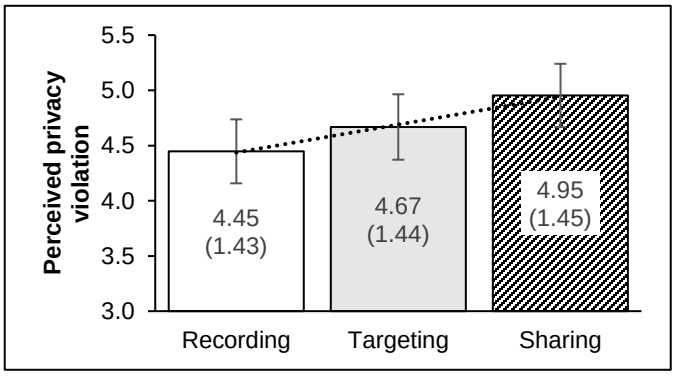
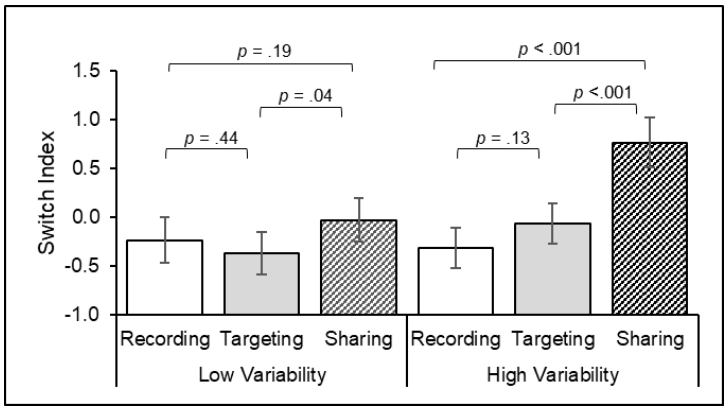


Figure 2. Study 2 Pretest: Linear trend of violation type on perceived privacy violation



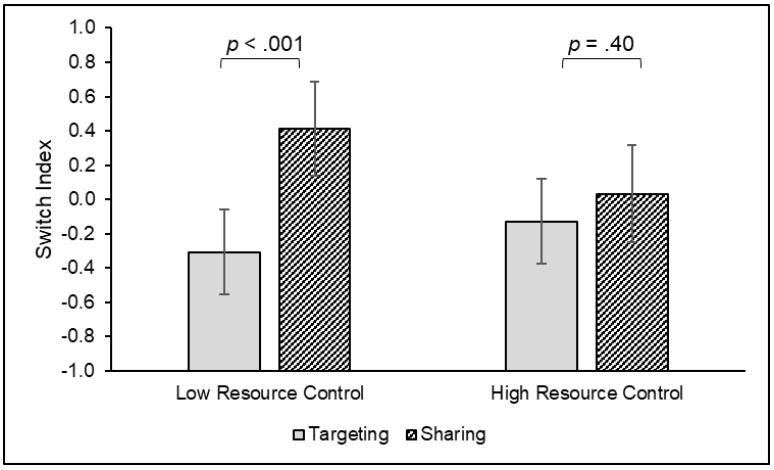
Notes: Means (SDs) provided within columns; error bars represent 95% CI

Figure 3. Study 2: Interaction of violation type and industry variability on switching behavior



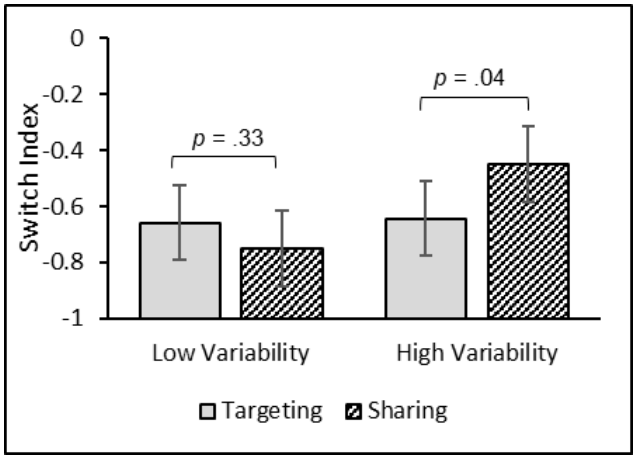
Notes: *p*-values represent planned contrast effects; error bars represent 95% CI.

Figure 4. Study 3: Interaction of Violation Type and Resource Control on Switching



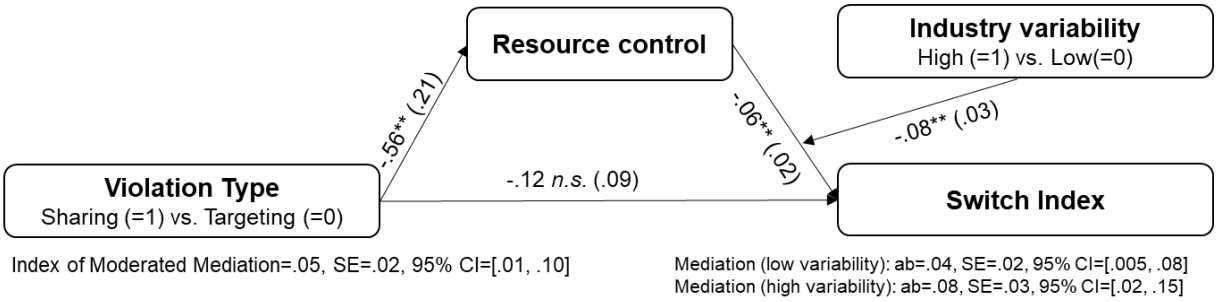
Notes: *p*-values represent planned contrast effects; error bars represent 95% CI.

Figure 5. Study 4: Effect of violation type and variability on switching behavior



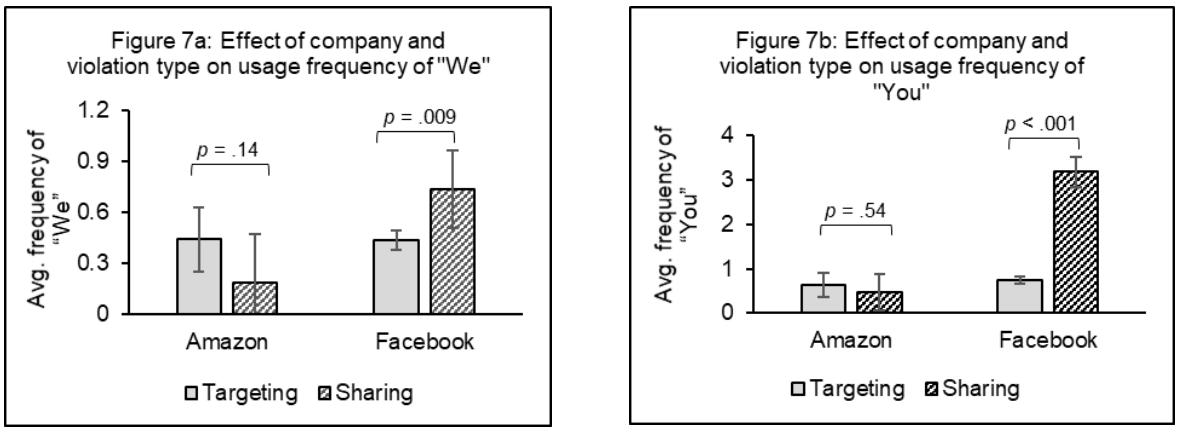
Note: *p*-values represent simple contrast effects; error bars represent 95% CI.

Figure 6. Study 4: Moderated Mediation Model



Notes: **$p < .01$; *n.s.* = not significant; coefficients (standard errors) are unstandardized

Figure 7. Study 5: Effect of company and violation type on usage frequency of "We" and "You"



Notes: *p*-values represent planned contrast effects; error bars represent 95% CI.