The Bulletproof Glass Effect: When Privacy Notices Backfire

Aaron R. Brough
David A. Norton
Leslie K. John

Working Paper 20-089
The Bulletproof Glass Effect: When Privacy Notices Backfire

Aaron R. Brough
Utah State University

David A. Norton
The Ohio State University

Leslie K. John
Harvard Business School

Working Paper 20-089
The Bulletproof Glass Effect: When Privacy Notices Backfire

AARON R. BROUGH
DAVID A. NORTON
LESLIE K. JOHN

Aaron R. Brough (aaron.brough@usu.edu) is Associate Professor of Marketing, Jon M. Huntsman School of Business, Utah State University, 3555 Old Main Hill, Logan, UT 84322. David A. Norton (norton.253@osu.edu) is a Visiting Assistant Professor, The Ohio State University, 500 Fisher Hall, 2100 Neil Ave Columbus, OH 43210. Leslie K. John (ljohn@hbs.edu) is Associate Professor of Business Administration, Harvard Business School, Harvard University, Baker Library 467, Soldiers Field Road, Boston, MA 02163. The authors thank Rebecca Walker Reczek and Joseph Goodman for their helpful comments on an earlier version of this manuscript and Holly Howe, Shannon Sciarappa, and Trevor Spelman for research assistance.
The Bulletproof Glass Effect: When Privacy Notices Backfire

ABSTRACT

Firms typically provide assurances to consumers about data management practices in the form of privacy notices. This manuscript proposes that ironically, such assurances can fuel rather than alleviate privacy concerns. Indeed, we show that consumers react to assurances as if they were warnings – a counterintuitive phenomenon because unlike warnings, which communicate danger, assurances are designed to communicate protection. Across one field experiment and five lab experiments, we show that a salient (vs. an absent or less salient) privacy notice can lead to decreased rather than increased purchase intent. This effect is mediated by consumer trust and is robust to the language in the privacy notice—it occurs even when the notice is overtly assuring, as well as when consumers see only a link to the notice but do not view its contents. The attenuation of the effect in joint (vs. separate) evaluation suggests that consumers’ hesitation to transact with organizations that have a salient privacy notice is not likely driven by an active aversion to assurances, but rather by the arousal of dormant privacy concerns.

Keywords: choice, purchase intent, privacy, privacy notices, warnings, assurances, trust, information disclosure
Consumers regularly encounter privacy notices explaining if and how their personal information will be collected, stored, used, and shared. In some industries and locations, privacy notices are mandated by law, but in others, companies choose whether to provide privacy notices. For example, an analysis of over one million apps in the Google Play Store between August 2017 and May 2018 found that approximately half (41.7%, 45.2%, and 51.8% on three separate crawls) included a privacy policy link (Story, Zimmeck, and Sadeh 2018). Even when notices are required, such as by Europe’s General Data Protection Regulation (GDPR), privacy policies are not uniformly salient. Some notices may include a detailed description of the company’s privacy practices, while others consist of merely a “privacy policy” hyperlink. In this research, we address the question of how such variation in the salience of privacy policies impacts consumers.

To consumers with active privacy concerns, the assurance offered by a privacy notice might be appealing for several reasons. First, privacy notices place legally-enforceable limits on how organizations can collect, store, use, and share consumers’ personal data. For example, the California Consumer Privacy Act (CCPA) allows consumers to sue companies that fail to fulfill promised privacy protections. Past research supports the notion that consumers favor restrictions on the gathering and use of personal information (Nowak and Phelps 1992)—particularly information that is highly sensitive (Milne et al. 2017). By knowing exactly what personal data companies have access to and understanding how it will be processed, consumers are expected to feel more comfortable providing personal data. Second, privacy notices often communicate security measures (e.g., encryption, firewalls) that are in place to protect consumer information from misuse. When such protections are not communicated via a strong privacy notice, consumers may respond defensively (Lwin, Wirtz, and Williams 2007), but transparency in how
a firm manages customer data can contribute to a reduction in customers’ perceived vulnerability (Martin, Borah, and Palmatier 2017). Third, in locations and industries where privacy notices are not legally required, the fact that a company voluntarily opts to disclose its data practices may signal that it is forthcoming and trustworthy. Indeed, companies’ respect of consumer privacy is closely linked to trust (Martin 2018; Martin and Murphy 2016). Historically, a lack of trust has been one of the leading reasons consumers are hesitant to shop online (Hoffman, Novak, and Peralta 1999a; 1999b) and explicit promises of fair information practices seem to attenuate consumers’ reluctance to share personal information with a firm (Culnan and Armstrong 1999).

Based on these reasons, a salient privacy notice might be expected to alleviate consumers’ concerns regarding potential abuses of personal data. Consistent with this line of reasoning, evidence from prior research shows that when a search engine prominently displayed privacy ratings for multiple websites, participants preferred to purchase from sites that offered higher levels of privacy protection (Tsai et al. 2011). Of course, privacy notices can differ in the level of privacy expectations they create and in the degree of assurance provided; some are more assuring than others (Martin 2015; Reidenberg et al. 2016). Still, one would expect consumers to place greater trust in a company that provides a privacy notice than one that does not.

In contrast to conditions where privacy concerns are already activated, in this research we examine conditions under which privacy concerns may be dormant. In this context, we argue that privacy notices, though designed to promote a sense of confidence that personal data will not be misused, can undermine consumer trust and decrease purchase intent (relative to a condition in which privacy assurances are either not provided or less salient). This is because privacy notices may activate privacy concerns that were previously dormant.
We refer to this phenomenon as the bulletproof glass effect, based on the idea that a privacy notice is analogous to bulletproof glass. Specifically, although bulletproof glass is designed for protection, its very presence may raise awareness of potential dangers and paradoxically cause consumers to feel more vulnerable than they would in its absence, holding constant the actual level of risk in the environment. By analogy, although privacy policies are designed to communicate protection, their very presence may raise awareness of potential dangers and paradoxically cause consumers to feel more uncomfortable and vulnerable than they would without any privacy assurances. Thus, both bulletproof glass and privacy notices may heighten concerns that might have otherwise remained dormant, leaving people feeling more vulnerable even when they are in fact more protected. In short, we argue that protections do not always produce an enhanced feeling of trust and in fact, may rouse the very concerns they are intended to assuage.

More broadly, in this research we examine the psychological processes that lead consumers to react similarly to assurances and warnings. Assurances and warnings, by definition, are designed to produce opposite outcomes: an assurance is intended to decrease concern by communicating protection, whereas a warning is intended to increase concern by communicating danger. In the following sections, we first review prior research on consumer privacy concerns. We then elaborate on our proposition that assurances and warnings, despite their opposing intended outcomes, can instead produce similar reactions among consumers with dormant privacy concerns.

*Consumer Privacy Concerns*
Faced with common news reports of identity theft, leaked personal data, and corporate security breaches, it is not surprising that consumers, businesses, and policy makers are concerned with protecting personal information from unauthorized access, collection, storage, use, and sharing (Hazel and Slobogin 2018; Kamleitner et al. 2018; Phelps, Nowak, and Ferrell 2000; White 2004). Moreover, the rapid growth of artificial intelligence and other forms of automation to collect and analyze consumer data is not always favorably received by consumers (Leung, Paolacci, and Puntoni 2018; Mende et al. 2019; Puntoni et al. 2019; Wertenbroch 2019). Consumers’ response to privacy threats is a function of both motivation and knowledge, and concern varies according to chronic privacy attitudes, information sensitivity, and context (Brough and Martin 2019).

Understanding consumers’ privacy concerns has consequential business implications and has been identified as an area ripe for consumer behavioral research (Lamberton and Stephen 2016). For example, consumers may react to the threat of privacy invasions in ways that affect profitability. Indeed, evidence suggests that as privacy concerns increase, purchase behavior decreases (Phelps, D’Souza, and Nowak 2001). Similarly, when consumers realize that personal information has been collected without consent, click-through rates drop sharply (Aguirre et al. 2015). One means of mitigating consumers’ concerns about the potential misuse of personal information is to provide a privacy notice.

Central to our theorizing is the notion that without some sort of stimulus, such as a privacy notice, privacy concerns are not always activated. Indeed, although many consumers express great concern over privacy threats, privacy concerns often remain dormant until triggered by the mention of privacy-related topics (Marreiros et al. 2017). Just as the act of measuring risky behavior can unintentionally increase the likelihood of engaging in the
behaviors (Fitzsimons and Moore 2008), we propose that providing a privacy notice can unintentionally activate consumers’ dormant privacy concerns.

Even when privacy concerns are at the forefront of consumers’ minds, they are often context-dependent and unstable across situations (Acquisti, Brandimarte, and Loewenstein 2015; Nissenbaum 2004; Smith, Dinev, and Xu 2011). Irrespective of stated preferences, consumers are quick to abandon privacy-protecting behaviors in response to small inconveniences or in exchange for small incentives (Athey, Catalini, and Tucker 2017). The malleability of privacy concerns is also manifest when participants’ likelihood to divulge sensitive information can be affected by factors as insignificant as the survey interface (John, Acquisti, and Loewenstein 2011) or the order in which questions are asked (Acquisti, John, and Loewenstein 2013). The inconsistency of consumers’ willingness to divulge sensitive information suggests that privacy concerns may be less influenced by objective risk factors and more influenced by the salience of cues that draw attention to risks.

Building on this notion, we argue that in a context where privacy concerns are not necessarily activated a priori, the mere presence of a privacy notice may in and of itself serve as a stimulus that brings privacy concerns to the fore, thus undermining rather than enhancing efforts to secure consumer trust and encourage the sharing of personal data. In other words, we expect assurances in this context to lead to a similar reaction among consumers as warnings, despite the fact that assurances and warnings have opposite intended outcomes. The next section will further elaborate on warnings versus assurances.

**Warnings versus Assurances**
Consumers regularly encounter both warnings and assurances. These warnings come in different forms (Stewart and Martin 1994), including warnings about false claims (Skurnik et al. 2005), advertisement disclaimers (Barlow and Wogalter 1993; Herbst et al. 2011; Johar and Simmons 2000), disclosures of conflict of interest (Cain, Loewenstein, and Moore 2011; Campbell, Mohr, and Verlegh 2013; Sah, Malaviya, and Thompson 2018), and product warning labels (Argo and Main 2004). Advocates of such warnings typically contend that by raising awareness of potential risks or dangers, the warning will prompt preventative action. Similarly, warnings in the privacy domain, such as the familiar notices displayed by web browsers: “the site ahead contains malware” or “this page is trying to load scripts from unauthenticated sources” are intended to raise awareness of privacy dangers so as to decrease trust and spur protective behavior; in this case, avoidance of the offending website.

Unlike warnings, assurances are intended to provide confidence that risk or danger has been mitigated, thus reducing concern while enhancing trust. Indeed, prior research suggests that privacy policies can be managed to create a positive customer experience (Goldfarb and Tucker 2013), and that even marginal improvements to privacy control and other online trust cues can increase consumers’ willingness to disclose sensitive information (Brandimarte, Acquisti, and Loewenstein 2013; Waldman and Mourey 2019). Rousseau et al. (1998) provide a widely accepted definition of trust as “a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another.” Consistent with this definition, we conceptualize trust in a privacy context as feeling comfortable with the way a firm will handle one’s personal information, as well as the extent to which consumers are willing to make themselves vulnerable by sharing personal information with a retailer.
Despite the opposing intended outcomes of warnings and assurances, we argue that they can instead produce similar reactions among consumers. Specifically, in a context where privacy concerns are not already activated, we predict that assurances can serve as cues that arouse privacy concerns. As a result, we predict that assurances paradoxically decrease rather than increase consumer trust, a response that would normally be associated with a warning.

Our account further implies that when privacy concerns are already activated, the absence of a privacy notice may be disconcerting. We posit such concerns to be active in a joint evaluation context in which one brand has a salient privacy notice and the other does not. Indeed, prior research has shown that compared to separate evaluation, joint evaluation can lead to comparative processing and increase attention to information that might otherwise be neglected (Hsee and Leclerc 1998; Hsee et al. 1999; Nowlis and Simonson 1997). Thus, we predict that the bulletproof glass effect will be attenuated in joint evaluation.

**Overview of Studies**

We tested these predictions in one field experiment and five lab studies. Specifically, study 1 is a field experiment that demonstrates the bulletproof glass effect by showing that increasing the salience of an assuring privacy notice reduced enrollment rates for a financial services firm. Study 2 provides a conceptual replication in the lab, showing that the presence (vs. absence) of a privacy notice can ironically decrease rather than increase purchase intent (and that this effect is mediated by consumer trust). Study 3 shows that despite the opposite outcomes they are designed to produce, both assurances and warnings can decrease consumer interest in a product. Study 4 shows that this effect influences downstream consequences, such that the presence versus absence of privacy notices changes consumers’ personal willingness to pay for a
product (without affecting their perception of the product’s value in the marketplace). Study 5 provides additional support for our theory that privacy notices arouse dormant privacy concerns by showing that the bulletproof glass effect is a function of the evaluation context and is more likely to be observed in separate rather than joint evaluation. Finally, study 6 uses a very conservative test in which mere awareness that a privacy policy exists, even when its content is not seen, is sufficient to decrease purchase intent and a behavioral manifestation of trust—willingness to disclose personal information. In all experiments we pre-set our sample sizes (or, in the case of the field experiment, the time period for data collection) and did not analyze the data until the target was met. We report all manipulations, measures, and data exclusions.

**STUDY 1**

In Study 1, we tested for the bulletproof glass effect. Specifically, we tested whether increasing the salience of an assuring privacy notice can backfire, diminishing consumers’ willingness to transact with a company.

*Method*

In this field experiment, we partnered with Borrowell, a Canadian financial technology firm with over one million users. To sign-up for Borrowell’s service, visitors must complete a nine-step enrollment process that involves providing sensitive personal information (e.g., name, address, birthdate, phone number, income, financial goals, and access to credit report).

The experiment was conducted among 15,864 prospective customers during a seven-day period in May 2019. Each prospective customer who visited the site was randomly assigned to
one of two conditions (Privacy Notice Salience: High vs. Low). In the Low-Salience condition, Borrowell’s privacy notice consisted of a hyperlink to its privacy policy on the first screen of the sign-up process. In the High-Salience condition, the link was preceded by a salient assurance of Borrowell’s commitment to the protection of customers’ personal information (see appendix for stimuli). The notice specified practices used to safeguard personal information (e.g., “bank-level encryption”) promised never to share information without consent, and explained how personal information would be used to benefit customers. To measure how the salience of the privacy assurance impacted prospective customers, we assessed conversion rates (i.e., the number of prospective customers who completed the enrollment process to sign-up for the service).

Results and Discussion

This study provided an initial demonstration of the bulletproof glass effect by showing that despite the explicit promise of protection it offered, the High-Salience privacy notice resulted in significantly fewer prospective customers choosing to sign-up for the service. As predicted, enrollment was 41.48% (3,265 / 7,872) in the Low-Salience condition but decreased to 39.66% (3,170 / 7,992) in the High-Salience condition; $\chi^2(1) = 5.45; p = .020$. Although this effect is rather small, it is meaningful—the fact that such a subtle manipulation could significantly change conversion rates at all is notable—especially considering that this was real behavior among actual customers. Moreover, when scaled across all prospective customers, even a small improvement to enrollment rates can have substantial financial ramifications.

This evidence suggests that, consistent with our theorizing, the increased salience of the privacy assurance decreased prospective customers’ interest in transacting with Borrowell. In the
next set of studies, we will provide a conceptual replication of the bulletproof glass effect in the lab and explore its underlying mechanism and boundary conditions.

**STUDY 2**

In this study, we aimed to provide a conceptual replication of the bulletproof glass effect by showing that a privacy notice, instead of promoting a sense of confidence that personal data will not be misused, can ironically decrease consumer trust and purchase intent (relative to a condition in which no privacy notice is provided).

*Method*

We recruited 200 participants (37.3% female; mean age = 35.41 years) on Amazon Mechanical Turk. Participants were randomly assigned to one of two conditions (Privacy Notice: Absent vs. Present). All participants were shown an identical image and description of a product (see appendix for stimuli).

In the Privacy Notice Absent condition, participants then proceeded directly to the dependent measures. In the Privacy Notice Present condition, participants were asked to click on a link to the retailer’s privacy policy before answering some questions about the product. The privacy notice, presented on the next screen, was crafted using language (adapted for length) from the actual privacy notices of two large clothing retailers (Nordstrom and Macy’s).

The dependent measures consisted of two items: purchase intent (How interested in purchasing this product would you be?) and trust (For this purchase, how comfortable would you be with the way your data will be collected and stored?), each measured using a sliding scale
ranging from 0 = Not at all to 100 = Extremely. We created this measure of trust based on Rousseau et al.’s (1998) widely accepted definition of trust as “a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another.” Thus, our trust item reflects the idea that it takes a certain degree of trust in order to feel comfortable with the way a firm will handle one’s personal information. Following the dependent measures, participants indicated their age and gender.

**Results**

In contrast to the typical belief that being transparent about practices relating to the collection, storage, and use of private information will increase consumers’ trust, we predicted that consumers who saw a privacy notice would feel less rather than more comfortable with the way their data was being used compared to participants who did not see a privacy notice, and that this would translate into lower purchase intent. As predicted, purchase intent was significantly lower when the privacy notice was present ($M = 26.56; SD = 27.61; N = 100$) versus absent ($M = 47.85; SD = 29.40; N = 100$); $t(198) = 5.28; p < .001$. Similarly, trust was also significantly lower when the privacy policy was present ($M = 27.16; SD = 30.17; N = 98$) versus absent ($M = 57.40; SD = 29.73; N = 100$); $t(196) = 7.10; p < .001$. To determine if trust mediated the effect of the privacy policy on purchase intent, we conducted a bias-corrected mediation analysis using PROCESS Model 4 (Hayes 2012). The mean indirect effect was negative ($a \times b = -15.15$) with a 95% confidence interval excluding zero (-21.22 to -9.73), indicating significant mediation.

**Discussion**
This study replicated the bulletproof glass effect observed in study 1 and also provided some initial evidence that reduced trust is the underlying mechanism. Specifically, the results showed that via lower trust, the mere presence (vs. absence) of a privacy notice can decrease consumers’ interest in purchasing a product. One potential explanation for the effect observed in both studies 1 and 2 is that the privacy notice provided additional information. To address this alternative explanation, in the next study we carefully designed a privacy notice such that it did not contain additional information relative to what shoppers could reasonably infer from viewing the description of product features. Study 3 also enabled us to directly compare the effect of a privacy notice on purchase intent to that of a warning.

**STUDY 3**

In study 3, we tested whether consumers react similarly when presented with a privacy notice versus a warning about the potential misuses of personal data. Despite the fact that unlike warnings, assurances are designed to communicate protection, we anticipated that a privacy notice would reduce purchase intent and trust to a similar extent as a warning.

**Method**

We recruited participants on Amazon Mechanical Turk. After completing an unrelated study, 802 participants (43.4% female; mean age = 34.30 years) were randomly assigned to one of six conditions in a 2 (Privacy Notice: Absent vs. Present) x 3 (Prime: Warning, Neutral, No Prime) between-participants design.
To test the effect of a warning on consumer trust and purchase intent, we presented participants in the Warning Prime condition with an article warning them of the potential abuses of geolocation data. As a control condition, participants in the Neutral Prime condition read an article discussing innovative technology in cars. The primes were based on real news articles published in *Forbes*, but modified to be similar in length and readability (see appendix for stimuli). As an alternate version of the control condition, participants in the No Prime condition did not read an article.

Following the prime manipulation, all participants were asked to imagine that they were considering a new technology system for their car and shown a description of a new product (called ViewTech), followed by detailed descriptions of various product features. As a test of the effect of a privacy notice on consumer trust and purchase intent, participants in the “Privacy Notice Present” condition viewed a privacy notice immediately before the detailed descriptions of product features, whereas participants in the “Privacy Notice Absent” condition did not view a privacy notice at all.

The privacy notice was designed to make explicit the same information that was already more subtly conveyed through the description of product features. For example, the privacy notice stated that the exact location of car and mobile devices will be collected and stored. This information may be reasonably and easily inferred from the product features, which include the ability to pinpoint your car’s exact location and retrace routes, to stream real-time route data to any mobile device for a live-updating map, and to receive directions to your parked car on your mobile device.

To verify that the privacy notice provided no additional information, we conducted a pre-test in which all participants (N = 101) viewed the product features, but only half viewed the
privacy notice. Participants were then asked seven binary questions (see appendix) about the collection, storage, and sharing of personal data. A tally of responses to these questions, where a total of seven indicates a perfectly accurate score, showed that participants’ understanding of privacy-related information was fairly accurate overall and, more critically, did not differ significantly across conditions ($M_{Present} = 6.27$ vs. $M_{Absent} = 6.06$); $t(99) = .83; p = .41$.

Next, purchase intent was measured by asking participants to indicate their level of interest in purchasing the product using a sliding scale (0 = Not at all interested; 100 = Very Interested). Consistent with study 2, trust was measured by asking participants how comfortable they would be with their data being collected and stored by ViewTech; participants indicated their response using a sliding scale (0 = Not at all comfortable; 100 = Extremely comfortable). As an attention check, participants were shown the headlines of both articles and asked to indicate which one they had read earlier in the study, or whether they had not read an article at all. Finally, participants reported demographics including gender, age, education, nationality, race, and income.

**Results**

For ease of interpretation, we combined the two control conditions (Neutral Prime and No Prime) because they did not differ statistically from one another (the non-collapsed analysis is reported in the appendix). A similar pattern of results was observed regardless of whether respondents who failed the attention check were included or excluded, so all participants were included in the analysis.

**Purchase Intent.** As predicted, an ANOVA revealed a main effect of privacy notice on purchase intent; $F(1,798) = 28.70; p < .001; \eta^2_p = .04$ as well as a main effect of prime; $F(1,798)$
= 23.21; \( p < .001; \eta^2_p = .03 \). No interaction effects were observed; \( F(1,798) = .21; p = .645 \).

Simple effects showed that in the combined control prime condition, the presence of a privacy notice decreased purchase intent (\( M_{Policy} = 59.57; SD = 32.21; N = 262 \) vs. \( M_{NoPolicy} = 72.82; SD = 25.29; N = 272 \)); \( F(1,798) = 25.33; p < .001; \eta^2_p = .03 \). Similarly, in the warning prime condition, the presence of a privacy notice decreased purchase intent (\( M_{Present} = 49.65; SD = 34.97; N = 133 \) vs. \( M_{Absent} = 60.80; SD = 31.43; N = 135 \)); \( F(1,798) = 9.00; p = .003; \eta^2_p = .01 \).

Consistent with the notion that privacy concerns often remain dormant until consumers are prompted to think about them, purchase intent was highest in the condition with neither a privacy policy nor a warning prime. Purchase intent was reduced to a similar extent by a warning or a privacy notice. The lowest purchase intent was in the condition where participants saw both a warning prime and a privacy policy, suggesting that the combination served as a double-alarm to raise concern. These results are illustrated in Figure 1.

[INSERT FIGURE 1 ABOUT HERE]

**Consumer Trust.** A similar pattern was observed for consumer trust. Specifically, an ANOVA revealed a main effect of privacy notice on trust; \( F(1,798) = 22.99; p < .001; \eta^2_p = .03 \) as well as a main effect of prime; \( F(1,798) = 14.63; p < .001; \eta^2_p = .02 \). No interaction effects were observed; \( F(1,798) = .48; p = .49 \). Simple effects showed that in the control condition, the presence of a privacy notice decreased trust (\( M_{Present} = 37.89; SD = 31.89; N = 262 \) vs. \( M_{Absent} = 50.19; SD = 28.06; N = 272 \)); \( F(1,798) = 22.53; p < .001; \eta^2_p = .03 \). Similarly, in the warning condition, the presence of a privacy notice decreased trust (\( M_{Present} = 30.86; SD = 30.17; N = 133 \) vs. \( M_{Absent} = 40.06; SD = 29.51; N = 135 \)); \( F(1,798) = 6.32; p = .012; \eta^2_p = .01 \).
**Mediation.** As in study 2, a mediation analysis using PROCESS Model 4 (Hayes 2012) showed that trust mediated the effect of a privacy notice on consumers’ purchase intent. The mean indirect effect was negative \((a \times b = -5.77)\) with a 95% confidence interval excluding zero \((-9.53 \text{ to } -4.22)\), indicating significant mediation.

Together, these results suggest that not only can a privacy notice decrease rather than increase consumers’ trust, it can also negatively affect interest in purchasing a product (similar to a warning).

**Discussion**

The first three studies have shown that the salience, and even mere presence (vs. absence), of a privacy notice can decrease consumers’ trust and interest in purchasing a product. However, it is not clear whether this is a halo effect that negatively influences all judgments about the product (e.g., expected retail value) or whether it is limited to decreasing a user’s personal interest in purchasing the product (e.g., willingness to pay).

In the next study, to assess the extent to which a privacy notice influences the perceived value of a product, we collected some additional measures (expected retail value and willingness to pay). We expected that privacy concerns would not impact market-level valuation (e.g., the expected retail value of a product, or what one thinks others would pay), but that they would affect individual-level valuation (e.g., a consumer’s own willingness to pay).

**STUDY 4**
This study aimed to show that the bulletproof glass effect influences downstream consequences, such that the presence versus absence of a privacy notice can change a consumer’s personal valuation of a product (without affecting perceptions of the product’s value in the marketplace). Second, we also aimed to provide additional evidence of the proposed psychological process underlying the bulletproof glass effect (i.e., decreased trust). Finally, we also tested the robustness of the bulletproof glass effect; specifically, whether it is robust to the timing of exposure to the privacy policy.

Method

Data for this study were collected from participants recruited on Amazon Mechanical Turk. After completing an unrelated study, 767 participants (47.7% female; mean age = 35.9 years) were randomly assigned to one of four conditions in a 2 (Privacy Notice Before Descriptions: Present vs. Absent) by 2 (Privacy Notice After Descriptions: Present vs. Absent) between-participants design. As in study 2, all participants were asked to imagine that they were considering a new technology system for their car and shown a description of a new product, followed by detailed descriptions of various product features. The product description and feature descriptions were identical to those used in study 2, as was the privacy notice. Depending on their condition, participants viewed the privacy notice immediately before the feature descriptions, immediately after the feature descriptions, both before and after the feature descriptions, or not at all.

Participants then indicated their purchase intent using the same scale as in study 2 and were asked to briefly explain the rationale for their answer. Next, participants estimated the retail price of the package (on a sliding scale from $1 to $10,000) and indicated their own willingness
to pay in a text box. Trust was measured using the same scale as in study 2. As an attention check, participants were shown a list of nine product feature descriptions and asked to identify the one they had NOT seen earlier in the study. Finally, participants reported demographics including gender, age, education, nationality, race, and income.

**Results**

The three conditions in which the privacy policy was present enabled us to test for possible recency or primacy effects; since no significant difference between these conditions was observed on any of the dependent measures, they were collapsed into a single condition for ease of interpretation (the non-collapsed analysis is reported in the appendix). Thus, in the analysis below we compare simply whether the privacy notice was present (before the product features, after the product features, or both before and after the product features) or absent. Because a similar pattern of results was observed regardless of whether respondents who failed the attention check were included or excluded, all participants were included in the analysis.

**Purchase Intent.** Replicating our earlier findings, we observed the bulletproof glass effect. Specifically, purchase intent was lower among participants who saw a privacy notice ($M = 55.67; SD = 34.15; N = 572$) than among those who did not ($M = 67.32; SD = 31.63; N = 195$); $F(1,765) = 17.55; p < .001; \eta^2 = .02$. We next analyzed the rationale participants provided for their interest in purchasing the product. Consistent with our theorizing that the bulletproof glass effect occurs due to the heightened attention to privacy concerns aroused by a privacy notice, participants who saw a privacy notice were significantly more likely to mention privacy-related thoughts in the decision rationale (43.9%; 251 of 572) than participants who did not see a privacy notice (7.2%; 14 of 195; $Z = 9.31, p < .001$).
**Consumer Trust.** A similar pattern was observed for consumer trust; participants who saw a privacy notice reported a lower level of trust ($M = 33.80; SD = 31.49; N = 572$) than participants who did not see a privacy notice ($M = 47.42; SD = 31.41; N = 195$); $F(1,765) = 27.23; p < .001; \eta^2_p = .03$. To determine if trust mediated the effect of the privacy notice on consumers’ interest in purchasing the product, we conducted a bias-corrected mediation analysis using PROCESS Model 4 (Hayes 2012). The mean indirect effect was negative ($a \times b = -9.01$) with a 95% confidence interval excluding zero (-12.68 to -5.65), indicating significant mediation.

**Willingness to Pay.** Moreover, participants who saw a privacy notice were willing to pay less for the product (Median = $800; M = $1,958; SD = $3,479; N = 557$) than participants who did not (Median = $1,500; M = $2,519; SD = $4,521; N = 188$), although this effect was only marginally significant $F(1,743) = 3.11; p = .078; \eta^2_p < .01$. After removing outliers that were more than two standard deviations above the mean in each condition, this effect also became significant; $F(1,715) = 8.75; p < .01; \eta^2_p = .01$. Together, these results provide evidence of the bulletproof glass effect by showing that not only can a privacy notice decrease rather than increase consumers’ trust, it can also negatively affect interest in and willingness to pay for a product.

**Estimated Retail Price.** Importantly, our manipulation did not affect expected retail prices; these did not differ regardless of whether the privacy notice was absent (Median = $3,015; M = $3,769; SD = $2,873; N = 195$) or present (Median = $3,014; M = $3,907; SD = $3,146; N = 572$); $F(1,765) = .29; p = .59; \eta^2_p < .01$. Viewed in light of the significant difference on the other measures, this null result suggests that the presence or absence of a privacy notice selectively influences the extent to which an individual consumer personally desires a product, but not the consumer’s perception of the objective value of the product in the marketplace.
Finally, we compared participants’ perceptions that the product would retail at a premium relative to their individual willingness to pay; by subtracting WTP from the expected retail price, we calculated a “retail premium” for each individual. This retail premium was significantly higher among participants who saw a privacy notice than among participants who did not; $F(1,743) = 4.36; p < .05; \eta_p^2 = .01$. In short, the privacy notice lowers consumers’ own willingness to pay for a product, but not their estimate of its retail value.

Discussion

This study provided converging evidence that privacy notices can decrease rather than increase consumer trust. It further showed that although the presence of a privacy notice tends to reduce an individual customer’s willingness to pay, it does so without affecting the individual’s expectation of the product’s retail value. These results suggest that rather than causing a negative halo-effect on all product judgments, privacy notices instead selectively reduce an individual’s willingness to pay for a product by increasing attentiveness to privacy concerns, and that this effect is mediated by a decrease in trust prompted by the presence of a privacy notice.

Although prior research suggests that the timing of soliciting sensitive information influences perceived intrusiveness (Acquisti, John, and Loewenstein 2012), we found that in a context where no sensitive information is being solicited, the timing of exposure to a privacy notice seems to matter less. In particular, our results suggest that introducing the privacy notice before versus after the product features (or both) did not affect trust. Instead, it was the presence versus absence of a privacy notice that decreased trust and willingness to pay.

In the next study, we aimed to show a boundary condition for the bulletproof glass effect. Specifically, we attribute the effect to dormant privacy concerns when a notice is absent but
heightened attention to privacy concerns when a notice is present. If our theorizing is correct, then in a joint evaluation context, where comparative processing makes the absence of a privacy notice more salient and activates privacy concerns, the bulletproof glass effect should be attenuated.

**STUDY 5**

Study 5 aims to replicate the bulletproof glass effect in separate evaluation, but show that it is attenuated in joint evaluation (when privacy concerns are activated due to comparative processing). By identifying a boundary condition for the bulletproof glass effect, we provide organizations with a strategy to present a privacy notice without compromising consumer trust.

Our expectation was that in separate evaluation, we would replicate the bulletproof glass effect observed in earlier studies, in that the presence (versus absence) of a privacy notice would result in lower trust. However, in joint evaluation, where privacy concerns are activated by exposing all participants to a company with a privacy notice, we expected that the bulletproof glass effect would be attenuated.

**Method**

We recruited 403 participants from Amazon Mechanical Turk (47.1% female; mean age = 35.05 years) who were randomly assigned to one of three conditions. In the first condition, separate evaluation with a privacy notice absent, participants were asked to imagine that they needed to buy some new clothes and had found some items they liked on the website of a retailer with which they were previously unfamiliar. The second condition, separate evaluation with a
privacy notice present, was identical with one addition—participants were told that before proceeding to check-out, they noticed a privacy policy, and on the following screen they were shown the privacy notice used in study 2. In the third condition, joint evaluation, participants were told to imagine that they had found items they liked on the websites of two online retailers that they were not previously familiar with, and that before proceeding to check-out, they had noticed a privacy policy on one site, but could not find a privacy policy on the other site. They were then shown the same privacy notice as participants in the separate evaluation conditions.

As in previous studies, our dependent measures were purchase intent and trust. After viewing the privacy notice, participants in the separate evaluations conditions were asked to rate on two different sliding scales “how interested would you be in making a purchase from this retailer” and “how comfortable would you be with the way your personal data is collected and stored by this retailer” (0 = Not at all; 100 = Extremely). Participants in the joint evaluation condition completed the same set of dependent measures for both retailers. Finally, participants reported demographics including gender, age, education, nationality, race, and income.

Results

Consistent with our predictions, the bulletproof glass effect observed in our previous studies was replicated in separate evaluation but attenuated in joint evaluation. These results are illustrated in Figure 2.
**Purchase Intent.** Specifically, comparing the first two conditions (in which the presence of a privacy policy was manipulated between-participants), purchase intent was significantly lower for the retailer with the privacy notice \((M = 29.81; SD = 27.36; N = 134)\) than for the retailer without the privacy notice \((M = 56.40; SD = 22.87; N = 134)\); \(F(1,266) = 74.47; p < .001; \eta^2_p = .22\). By contrast, in joint evaluation (when the presence of a privacy notice was manipulated within-participant), purchase intent was not significantly lower for the retailer with the privacy notice \((M = 40.84; SD = 27.80; N = 130)\) than for the retailer without the privacy notice \((M = 43.08; SD = 27.68; N = 130)\); \(F(1,129) = .66; p = .419; \eta^2_p = .01\).

**Consumer Trust.** A similar pattern was observed for consumer trust. In separate evaluation, trust was significantly lower for the retailer with the privacy notice \((M = 25.39; SD = 27.56; N = 134)\) than for the retailer without the privacy notice \((M = 42.28; SD = 25.82; N = 134)\); \(F(1,266) = 26.80; p < .001; \eta^2_p = .09\). By contrast, in joint evaluation, trust was not significantly lower for the retailer with the privacy notice \((M = 33.76; SD = 28.13; N = 130)\) than for the retailer without the privacy notice \((M = 36.99; SD = 28.34; N = 130)\); \(F(1,129) = 1.345; p = .248; \eta^2_p = .01\).

**Discussion**

As expected, this study showed that the bulletproof glass effect observed in earlier studies was replicated in separate evaluation, but attenuated in joint evaluation. This result is consistent with our theorizing that in separate evaluation, when privacy concern is aroused by the mere presence of a privacy notice, consumers will, ironically, feel that their personal data is less secure than when no privacy notice is present and concerns remain dormant. The attenuation of the effect in joint evaluation provides an important boundary condition, suggesting that consumers’
hesitation to transact with organizations that have a salient privacy notice is not likely driven by an active aversion to assurances, but rather by the arousal of dormant privacy concerns that had not previously been activated.

Thus far, our studies have manipulated exposure to the content of a privacy notice. In the next study, we test whether the bulletproof glass effect is observed when participants are aware that a privacy notice exists, but do not view its content. This allows us to rule out any alternative explanations for the effect that are based on the specific content of the privacy policy. In addition to its theoretical import, this test also has practical value, since consumers do not always read privacy notices (Milne and Culnan 2004).

**STUDY 6**

This study had several objectives. First, to further assess the robustness of the bulletproof glass effect, we aimed to perform a conservative and rigorous test of our theory by designing an extra-assuring privacy notice that emphasized protection even more than the realistic privacy notices used in earlier studies. Specifically, though we designed previous studies with close approximations of real privacy policies from actual retailers for ecological validity, in this study we designed and pre-tested stimuli that convey even greater protection and assurance. Second, to provide additional process evidence, we added a third condition to the present versus absent conditions used in earlier studies. If privacy notices affect consumer trust and purchase intent by activating privacy concerns, then mere awareness of a privacy notice’s existence (even without exposure to its content) should be sufficient to activate privacy concerns and produce the bulletproof glass effect. Third, we also aimed to measure how a privacy notice impacts real
behavior by examining a behavioral measure of trust—whether participants exposed to a privacy notice are less likely to share identifying information.

**Pre-test**

We conducted a pre-test to assess the extent to which the privacy notices used across our studies are viewed as assuring. One hundred undergraduate students participated in this pre-test for extra credit. Participants were randomly assigned to one of two conditions (Realistic Privacy Notice vs. Extra-Assuring Privacy Notice). Participants in the Realistic Privacy Notice condition were shown the privacy notice used in Studies 2 and 5 (the one adapted from the actual privacy notice of Nordstrom and Macy’s). In the Extra-Assuring Privacy Notice condition, we made only minor changes (see appendix for stimuli). For example, we inserted the word “Protection” into the title, and changed every instance of “collect” in the Realistic Privacy Notice to “protect” in the new notice (e.g., “We collect personal information…” became “We protect personal information…”). Participants then indicated their agreement with six statements about the notice they saw (1=Strongly Disagree; 10= Strongly Agree). A factor analysis subsequently showed that these six statements loaded onto two factors: Assurance ($\alpha = .52$) and Clarity ($\alpha = .67$). The Assurance items were: “The policy makes me feel safe,” “The policy makes me feel protected,” and “The policy makes me feel comfortable in sharing my information.” The Clarity items were: “The policy is easy to understand,” “The policy is specific with respect to how my data will be used,” “The policy is specific with respect to how my data will be protected.”

The pre-test showed that in aggregate, both notices were rated higher than the midpoint, and that the Extra-Assuring Privacy Notice was rated even higher than the Realistic Privacy Notice ($M_{Extra-Assuring} = 7.30; SD = 0.86; M_{Realistic} = 5.91; SD = 1.03); $F(1,98) = 53.88; p < .001$. 
When comparing the subscales; the Extra-Assuring Privacy Notice was viewed as more assuring than the Realistic Privacy Notice ($M_{\text{Extra-Assuring}} = 7.05; M_{\text{Realistic}} = 6.07$); $F(1,98) = 12.15; p = .001$; as well as more clear ($M_{\text{Extra-Assuring}} = 7.54; M_{\text{Realistic}} = 5.75$); $F(1,98) = 50.19; p < .001$.

Though the Extra-Assuring Privacy Notice is less ecologically valid, it represents a conservative test of our central proposition that exposure to a privacy notice, despite its assuring language, increases privacy concern and leads to lesser interest in purchase.

**Method**

Two hundred and ninety-eight undergraduate students at a large Midwestern University in the United States participated in this study for extra credit. Participants were randomly assigned to one of three conditions (Extra-Assuring Privacy Notice: Absent, Unseen, or Seen) in a between-participants design.

Using the same stimuli as in study 2, all participants were shown a product image and description. In the Seen condition, participants were asked to review the retailer’s privacy policy and were shown the Extra-Assuring Privacy Notice (see appendix for stimuli). In the Unseen condition, participants were similarly asked to review the retailer’s privacy policy, but when they clicked on the privacy policy link, they were shown a screen that mimicked an Internet browser screen which could not be properly loaded. Thus, participants in the Unseen condition were aware that the privacy notice existed, but did not view its contents. As with earlier studies, participants in the Absent condition were not asked to review, nor did they see a link to the retailer’s privacy notice. All participants then completed the same measures used in study 2 (purchase intent, trust, and demographics).
Finally, as a behavioral measure of willingness to disclose information, all participants were told that the retailer “may wish to follow-up with survey respondents to clarify your responses to this survey.” To facilitate this re-contact, they were asked if they would be willing to provide personal contact information (e.g., name, address, email address, phone number) to the retailer. It was emphasized that doing so was entirely voluntary and that the online contact form could be completed in less than two minutes. Participants then responded either “Yes, take me to the form” or “No Thanks.” Following this measure, participants were taken to a debrief page where they were informed of the study’s intent and no identifiable information was actually collected, in accordance with IRB protocol.

**Results**

*Purchase intent.* An ANOVA revealed a main effect of privacy notice on purchase intent \( (F(2,295) = 6.24, p < .01, \eta_p^2 = .04) \) such that purchase intent was lower in the Seen \( (M_{seen} = 36.71, SD = 16.24, N = 101; \ t(199) = 2.11, p = .036) \) and Unseen \( (M_{unseen} = 33.18, SD = 17.31, N = 97; \ t(195) = 3.35, p < .01) \) conditions than in the Absent condition \( (M_{absent} = 42.15, SD = 20.16, N = 100) \). The two conditions where a privacy notice was present (Seen and Unseen) did not significantly differ \( (t(196) = 1.48, p = .139) \). These results are illustrated in Figure 3.

*Consumer Trust.* Similarly, an ANOVA revealed a main effect of privacy notice on consumer trust \( (F(2,295) = 6.265, p < .01, \eta_p^2 = .04) \) such that trust was lower in the Seen \( (M_{seen} = 36.44, SD = 17.37, N = 101; \ t(199) = 3.39, p = .001) \) and Unseen \( (M_{unseen} = 40.11, SD = 19.01, \)
$N = 97; t(195) = 2.06, p = .041$) conditions than in the Absent condition ($M_{\text{absent}} = 46.55, SD = 24.41, N = 100$). The two conditions where a privacy notice was present (Seen and Unseen) did not significantly differ ($t(196) = 1.42, p = .157$).

*Behavioral Measure.* As predicted, a significant difference was observed across conditions in participants’ willingness to disclose personal information, $\chi^2 (2, N = 298) = 21.23, p < .001$. Specifically, more participants in the Absent condition (33.0%; $N = 33 / 100$) were willing to disclose personal information than in the Unseen (10.3%; $N = 10 / 97$) and Seen (11.9%; $N = 12 / 101$) conditions. These results are illustrated in Figure 4.

**Discussion**

This study provided an additional demonstration of the bulletproof glass effect by showing that even strong assurances, such as an extremely protective privacy notice, decrease consumers’ interest in a product. Moreover, this effect occurs even when the contents of the notice are not viewed, suggesting that mere awareness of the existence of a privacy notice is sufficient to activate privacy concerns. Importantly, the replication of the effect in the Unseen (vs. Absent) condition rules out any alternative explanations based on the specific content or length of the privacy notice. Further, the results of our behavioral measure showed that provision of a privacy notice decreased the likelihood of sharing personal contact information. These results are consistent with our theorizing that a salient privacy notice may arouse privacy concern.
and lead people to subsequently engage in protective behavior (e.g., choosing not to make a purchase or disclose personal information).

**GENERAL DISCUSSION**

Although one would expect consumers to place greater trust in companies that have salient privacy notices than those that do not, our results suggest the opposite—that salient privacy notices, independent of their content, can undermine trust and potentially hurt sales. We compare privacy notices to bulletproof glass, which is designed for protection, yet by its mere presence may focus attention on potential dangers and paradoxically cause consumers to feel less safe than they would without it. Similarly, although privacy notices are assurances designed to communicate protection, we propose that they can decrease both consumers’ trust and their interest in purchasing a product. Importantly, we focus on how mere exposure to a privacy notice can affect consumers even when personal data has not yet been collected, used, or shared; additional factors, such as a firm’s violation of privacy notices, may further undermine consumer trust (Martin 2016). Our findings highlight conditions under which consumers process assurances as warnings and provide new insights regarding persuasion and the drivers of consumer trust.

*Theoretical Contributions*

From a theoretical standpoint, this research highlights parallels between the unintended ways in which consumers react to warnings and assurances; we show that like warnings, assurances can paradoxically backfire. Just as some warnings, contrary to their overt intentions, increase
rather than decrease consumer trust, we identify situations in which assurances, contrary to their overt intentions, decrease rather than increase consumer trust. Indeed, prior research suggests that warning messages do not always achieve their intended effects, sometimes failing to increase consumer compliance (Menon, Block, and Ramanathan 2002) or even resulting in greater acceptance of the false claims that people were warned against (Skurnik et al. 2005). Consumers seem to trust advisors who disclose conflicts of interest (Cain, Loewenstein, and Moore 2011; Sah, Malaviya, and Thompson 2018) and tend to be more persuaded by messages that include negative information (Ein-Gar, Shiv, and Tormala 2012; Herr, Kardes, and Kim 1991; Ward and Brenner 2006). One mechanism that has been identified in the persuasion literature for these kinds of effects is peripheral (versus central) processing (Sah, Malaviya, and Thompson 2018). In a complementary fashion, we argue that privacy notices do not always achieve their intended effects to be assuring and can be disconcerting rather than comforting when privacy concerns are dormant.

Moreover, our findings illustrate a situation in which consumers seem to respond more favorably to omission than transparency. This is conceptually related to the body of consumer research on information avoidance (Sweeny et al. 2010), which shows that consumers often prefer ignorance to bad news. For example, “the ostrich effect” describes the tendency of investors who receive preliminary bad or ambiguous news to shield themselves from further news by monitoring their accounts less rather than more frequently (Karlsson et al. 2009). One difference, of course, is that privacy notices are intended to convey good rather than bad news, but this is now always how they are perceived by consumers. The negative reaction we observed to transparency in the context of privacy notices also extends prior work showing negative reactions to transparency (vs. imprecision) in the context of marketing communications (Isaac, Brough, and Grayson
2016). Nonetheless, the attenuation of the bulletproof glass effect observed in joint evaluation suggests that consumers’ hesitation to transact with organizations that have a salient privacy notice is not likely driven by an active aversion to assurances, but rather by the arousal of previously dormant privacy concerns. This interpretation is consistent with the notion that privacy concerns (and the lack thereof) are context-dependent (Acquisti, Brandimarte, and Loewenstein 2015; Acquisti, John, and Loewenstein 2013, John, Acquisti, and Loewenstein 2011; Athey, Catalini, and Tucker 2017) and often remain dormant until consumers are prompted to think about them (Marreiros et al. 2017).

Our findings that privacy policies impact trust also extend prior work on how formal contracts may undermine trust (Martin 2016; Poppo and Zenger 2002; Puranam and Vanneste 2009) and how confidentiality assurances may impact response rates among potential survey respondents (Singer, Hippler, and Schwarz 1992; Singer, Von Thurn, and Miller 1995). Whereas prior work suggests that assurances increase compliance when survey respondents are asked to provide sensitive personal data (Singer et al. 1992; 1995); our findings showed the opposite pattern—assurances decreased compliance when consumers were asked about their interest in purchasing a product or asked to disclose personal contact information. One possible explanation for this difference is that whereas Singer et al. (1992; 1995) examined how confidentiality assurances change expectations about the type of data that would be collected, we examine how privacy notices arouse concerns about how the data will subsequently be used. Future research may further explore how different forms of assurances (privacy vs. confidentiality), different dependent measures (trust and purchase intent vs. response rates) and different populations (online consumers vs. potential survey respondents) impact individuals’ responses to assurances.
Managerial and Policy Implications

This work also has important practical implications for businesses, consumers, and policy-makers. Transparency in data practices, and the lack thereof, has been the source of much debate. Many of the transformational technologies that are influencing both marketers and consumers at an unprecedented rate are deeply invasive of consumer privacy, but obfuscate privacy risks. Though regulators and consumer advocacy groups demand more transparency, our findings suggest that when businesses provide greater transparency, customers may react negatively. Indeed, our results show that consumers are more likely to transact with organizations that lack a privacy notice than with organizations that are transparent in providing one.

Our findings that mere awareness of the existence of a privacy notice—even when it is not viewed—can decrease interest in purchasing a product, reinforces the view of consumer privacy advocates that companies have an incentive not to provide greater transparency in how private consumer data is managed. This negative incentive may hinder compliance, and even if regulators enforce compliance it could lead to a climate of distrust as consumers’ perceptions of security are decreased rather than increased by the additional assurances. However, we also show that in joint evaluation when consumers engage in comparative processing, the bulletproof glass effect is attenuated, suggesting that companies wishing to provide assurances without undermining consumer trust may increase their chances of success through direct comparison to a competitor that is less transparent in its data practices. This also suggests that the negative impact of a salient privacy policy on consumer trust and purchase intent may be attenuated once privacy concerns have already been activated (e.g., among repeat customers).
REFERENCES


Puntoni, Stefano, Rebecca Walker Reczek, Markus Giesler, and Simona Botti (2019),
“Consumer AI: Dystopias and Counter-Mythic Strategies,” working paper, Rotterdam School of Management, Erasmus University.


FIGURE 1: LIKE WARNINGS, PRIVACY NOTICES CAN DECREASE PURCHASE INTENT (STUDY 3)

NOTE.—The presence (vs. absence) of a privacy notice lowered purchase intent in both the Control and Warning Prime conditions. Purchase intent is lowest when both a privacy notice and a warning prime are present.
FIGURE 2: JOINT EVALUATION ATTENUATES THE BULLETPROOF GLASS EFFECT OBSERVED IN SEPARATE EVALUATION (STUDY 5)

NOTE.—In separate evaluation, purchase intent was lower when a privacy notice was present rather than absent. However, this bulletproof glass effect was attenuated in joint evaluation.
FIGURE 3: PRIVACY NOTICES—SEEN OR UNSEEN—CAN DECREASE PURCHASE INTENT (STUDY 6)

NOTE.—Purchase intent was lower when a privacy notice was present (regardless of whether its contents were seen or unseen) versus absent.
FIGURE 4: PRIVACY NOTICES—SEEN OR UNSEEN—CAN DECREASE WILLINGNESS TO DISCLOSE PERSONAL INFORMATION (STUDY 6)

NOTE.—Fewer participants were willing to disclose personal contact information when a privacy notice was present (regardless of whether the contents of the policy were seen or unseen) than when a notice was absent.
WEB APPENDIX

Study 1 Stimuli

Low salience condition (link only)
High salience condition (concise privacy assurance + link)

It's fast and easy to get your free Equifax credit score!
Creating an account won't affect your credit!

**Privacy Policy**

Borrowell is committed to the protection of personal information (e.g., income, age, credit report) and we use bank-level encryption to keep it safe.

Borrowell would never share your information without your consent as laid out in our Privacy Policy (link).

Borrowell uses your information to obtain your Equifax credit report, provide you with personalized services, communicate with you and manage your account. It is also used on an anonymous basis for research and analysis to improve Borrowell services for you.

**Step 1: Create Account**

What is your email address?
test1552931988838@knowwhatwhen.com

Confirm your email address
test1552931988838@knowwhatwhen.com

Create a password
[
**********

At least 8 characters with at least 1 number

Confirm your password
[
**********

At least 8 characters with at least 1 number

By clicking Create Account, you agree to the Terms of Use and Privacy Policy.

Create Account

[Highlighting is for illustrative purposes only; text was not highlighted for customers.]
Study 2 Stimuli

In this study we are interested in your opinions and thoughts about potential new products on the market from an online retailer. You will randomly be presented with products that may be from a variety of industries (e.g., consumer electronics, food and beverage, travel, etc.). These are all real products available on the market, but brand names have been changed. Please read the description carefully and provide your honest opinion of the products you are presented.

This pair of sunglasses comes with a fashionable look that is made with durable plastic acetate for lighter weight and longer lasting wear. These sunglasses are the perfect accessory to complete any look. Featuring both classic and bright rubber fronts, metal temples and tone-on-tone temple tips. The oversized Round Sunglasses shape provides extra coverage and 100% UV protection, while the soft bridge adds a twist to this design. Personalize your style from a variety of frame colors and lens treatments including green gradient, grey gradient and brown gradient.

Privacy Notice Present Condition
Click below to read the retailer's Privacy Policy before you answer some questions about the item you saw.

Privacy Notice Absent Condition
[Blank]
Privacy Policy

Categories of Information We Collect
We collect personal information when communicating or interacting with you through our website or family of companies. Personal Information is any information that we can use to identify, locate, or contact you. Some examples of Personal Information we collect include:
- precise location information if you provide it to us (e.g., to show you the store nearest you)
- general location information from your browser or device (which we use for internal purposes, such as foot traffic analysis)
- contact information (e.g., name, email, phone, address) when you place an order
- financial information (e.g., credit or debit card number) when you make a purchase
- product preferences (e.g., when you browse our website, create a Wish List, complete Product Reviews, place an order, or make a return)
- physical characteristics (e.g., based on clothing size or when you are recorded by in-store cameras used for safety, security and operational purposes, such as to measure traffic patterns in our stores)

We may also collect personal information about you from other third parties, such as demographic firms, to make our future service and marketing efforts more efficient and personalized for you. We may combine all information we collect and we may disclose this information within our corporate family of companies or our service providers. When you visit our websites or other online services we may also gather certain information automatically and store it in log files. This information may include Internet Protocol (IP) addresses or other device identifiers, browser information, Internet Service Provider (ISP), operating system, location, date/time stamp and clickstream data.

Do We Share Your Information?
The information gathered may be shared with our family of companies. We also share the information with third parties, including responsible companies with which we have a relationship. We may share your personal information with unrelated outside companies so that they can directly market their products or services to you if we feel that a company offers products or services that we believe may be of interest.

Data Processing and Storage
We and our third party service providers may process or store your personal information outside of the United States. In accordance with the laws of those countries, in certain circumstances your personal information may be accessible by foreign law enforcement, regulatory bodies or other authorities.
Study 3 Stimuli

Warning Prime

**BEWARE: The Dangers of Location Data**

This week, California Attorney General Kamala Harris advised her constituents to disable location-tracking devices. Consumers likely don’t know that their phones, and sometimes even the devices in their cars’ infotainment systems, continuously track their location for reasons that have nothing to do with 911 requirements. Her advice is to turn on location tracking only for specific cases.

That is wise advice. Geolocation data (that is, the street and city where a phone or car is located at any moment) reveals intimate details about people’s lives—their visits to drug treatment clinics, psychiatrists, prospective employers, political events, churches, and more—information that is subject to serious abuse. From stalking to theft and discrimination, as AG Harris told USA Today, “Broadcasting your location can sometimes expose you and a family to risk of theft or physical harm.” For instance, you may be unknowingly revealing your location if your phone is “geotagging” your photos. Sharing a “selfie” without disabling geo-tagging can be dangerous, especially for victims of stalking or domestic abuse. Companies sell location information to data brokers, who compile consumers’ medical conditions, religious affiliations, and more.

There’s a reason people feel creeped out when they think someone is tracking their movements. Being followed is scary and invasive. Insurance companies may increase your premium if you speed or regularly drive through high-risk zones. Much worse, curious employees of the company collecting your data can learn about your trips to the cancer screening clinic, psychiatrist, plastic surgeon, AIDS treatment center, strip club, divorce attorney, union meeting, mosque, or synagogue from the safety of their office. Your personal, professional, religious, and sexual conduct becomes easy and inexpensive to track down.

Unethical employees can abuse this information to blackmail, harass, and threaten you, or even to break into your home when you aren’t there.

Location tracking technology constitutes a significant invasion of privacy. It has the potential to create permanent records of virtually everywhere you have driven, radically changing the consequences of leaving home to pursue private life. This information is often stored indefinitely, with few or no restrictions to protect privacy rights. It should not be collected or shared without express consent from consumers.

Neutral Prime

**The Future of In-Car Technology**

In the very near future, your dashboard may become as versatile as your laptop, with drivers taking the Internet along with them. With Head-Up Display (HUD) and active glass technology that can display vibrant images on a windshield, cars of the future will improve driver awareness and reduce distractions.

Imagine a navigation system that actually highlights the next turn (as seen from your perspective, through the windshield) as you approach it. Or computer sensors that darken the windshield in the exact spot where glare impacts drivers—a monumental improvement over the current rearview sun visor. And the rapid increase in external sensor technology will enable fully autonomous driver override systems, without human oversight, in certain circumstances. The advent of electric vehicles will forever change how automobiles connect with infrastructure. A traffic management system, tricked out with cameras and computers to record and analyze the road, will provide instructions to facilitate traffic decongestion.

Currently, in-car technology is hardware-based, with upgrades requiring new physical installation; to play satellite radio or use navigation, an aftermarket unit or option from the automaker must be purchased. In the near future, however, upgrades will merely require new software. A few manufacturers such as Audi, BMW, and Ford have started experimenting with connected cars in their latest models. But soon, most new cars will become rolling Wi-Fi hot spots, either sharing an Internet connection with a “smartphone” (called “tethering”) or with a separate, dedicated data plan. In five years, nearly 25 percent of cars will be connected to the Internet, which will transform in-car entertainment.

“Think of your computer pre- and post-dialup,” Robinson says. Since a mouse and a keyboard would be difficult to use at highway speeds, the most advanced setups will tailor the Web for an in-car experience. When connected to the Internet, cars would use voice-recognition software and specially designed applications that allow drivers and passengers to listen to music via Pandora and keep in touch with social networks like Twitter while on the road. A simplified representation of the route could be streamed to the back seat, and passengers could search menus of nearby restaurants and receive discounts. Wi-Fi’s potential will be limited only to the imaginations of software developers.

No Prime

[Blank]
FutureCar™ by ViewTech

ViewTech’s innovative technology is designed to make your life easier. Our FutureCar™ package seamlessly integrates a sleek in-car navigation system, off-the-grid geolocation, a cutting-edge mobile app, and location-based alerts and offers to provide you with benefits you’ve only read about in science fiction novels.

PRIVACY POLICY

Information We Receive
We collect and store precise, real-time data about:
- The exact location of your car and mobile devices
- Your route history
- The time you enter and exit certain areas
- Your speed
- Locations you visit frequently

Data Sharing
We may share this information with third parties such as our partners and, by your consent, with other users.

Data Retention
We will retain your data for as long as you use the product.

Your Consent
By using this product, you are consenting to our collecting, storing, deleting, using, combining and disclosing your information as set forth in this Privacy Policy.
EFFORTLESS NAVIGATION
Driving directions superimposed directly onto your windshield.

NO MORE “ARE WE THERE YET?”
Stream real-time route data to any mobile device for a live-updating map.
ALWAYS KNOW YOUR PRECISE LOCATION

Pinpoint your car’s exact location and retrace routes, even on unmarked roads.

AVOID TRAFFIC JAMS

Receive alternate route suggestions BEFORE you become stuck in traffic.
WARNING: SPEED TRAP AHEAD

Windshield alerts warn you as you approach active radar while speeding.

Reduce speed to 60mph

ELIMINATE PARKING TICKETS

Track the exact time you arrive and leave a location and receive mobile alerts when a meter is about to expire.

Entry: 3:02pm  Exit: 3:28pm
DON’T FORGET THE MILK

Receive coupons from retailers on your mobile device when you frequently visit certain areas.

FEELING LOST?

Walk straight to your car with simple FindMyCar directions delivered instantly to your mobile device.
Study 3 Pre-Test

[Half of the participants viewed only the product description and features, and half also viewed the privacy notice. All participants were then asked the following seven binary questions.]

Now we would like you to answer a few questions. As a reminder, the product description is shown again at the bottom of this screen.

What personal information about you is collected when you use this product? (Select all that apply.)

☐ The exact location of your car and mobile devices
☐ Your route history
☐ The time you enter and exit certain areas
☐ Your speed
☐ Locations you visit frequently

Can your personal information be shared with third parties and, by your consent, with other users, when you use this product?

☐ Yes
☐ No

Will your personal information be retained for as long as you use this product?

☐ Yes
☐ No
Study 3 Non-Collapsed Analysis

**Purchase Intent.** As predicted, an ANOVA revealed a main effect of privacy notice on purchase intent; $F(1,796) = 34.10; p < .001; \eta^2_p = .04$ as well as a main effect of prime; $F(2,796) = 11.66; p < .001; \eta^2_p = .03$. No interaction effects were observed; $F(2,796) = .54; p = .580$.

Pairwise comparisons showed that the effect of the two Control Primes on purchase intent did not differ statistically from one another ($p = .812$) but that the Warning Prime led to significantly lower purchase intent than both the Neutral-Prime ($p < .001$) and No-Prime ($p < .001$) conditions. Specifically, in the absence of a privacy notice, the Warning Prime led to lower purchase intent than both Control Primes ($M_{\text{WarningPrime}} = 60.80; N = 135$ vs. $M_{\text{NeutralPrime}} = 71.30; N = 138$ vs. $M_{\text{NoPrime}} = 74.39; N = 134$). Likewise, in the presence of a privacy notice, the Warning Prime led to lower purchase intent than both Control Primes ($M_{\text{WarningPrime}} = 49.65; N = 133$ vs. $M_{\text{NeutralPrime}} = 60.50; N = 129$ vs. $M_{\text{NoPrime}} = 58.67; N = 133$).

**Consumer Trust.** A similar pattern was observed for consumer trust. Specifically, an ANOVA revealed a main effect of privacy notice on trust; $F(1,796) = 28.26; p < .001; \eta^2_p = .03$ as well as a main effect of prime; $F(2,796) = 7.43; p < .001; \eta^2_p = .02$. No interaction effects were observed; $F(2,796) = .30; p = .743$. Pairwise comparisons showed that the effect of the two Control Primes on trust did not differ statistically from one another ($p = .631$) but that the Warning Prime led to significantly lower purchase intent than both the Neutral-Prime ($p < .001$) and No-Prime ($p = .002$) conditions. Specifically, in the absence of a privacy notice, the Warning Prime led to lower trust than both Control Primes ($M_{\text{WarningPrime}} = 40.06; N = 135$ vs. $M_{\text{NeutralPrime}} = 50.36; N = 138$ vs. $M_{\text{NoPrime}} = 50.01; N = 134$). Likewise, in the presence of a privacy notice, the Warning Prime led to lower trust than both Control Primes ($M_{\text{WarningPrime}} = 30.86; N = 133$ vs. $M_{\text{NeutralPrime}} = 38.98; N = 129$ vs. $M_{\text{NoPrime}} = 36.83; N = 133$).
Study 4 Non-Collapsed Analysis

*Purchase Intent.* Replicating our earlier findings, we observed the bulletproof glass effect. Specifically, purchase intent was lower among participants who saw a privacy notice, whether before, after, or both before and after the product features \((M_{\text{Before}} = 55.20; N = 185 \text{ vs. } M_{\text{After}} = 57.29; N = 192 \text{ vs. } M_{\text{Both}} = 54.52; N = 195)\) than among those who did not see a privacy notice at all \((M_{\text{Absent}} = 67.32; N = 195)\). An ANOVA shows this difference to be significant; \(F(3,763) = 6.08; p < .001; \eta^2_p = .02\). We next analyzed the rationale participants provided for their interest in purchasing the product. Consistent with our theorizing that the bulletproof glass effect occurs due to the heightened attention to privacy concerns aroused by a privacy notice, participants who saw a privacy notice before (42.7%), after (38.0%), or both before and after (50.8%) the product features were significantly more likely to mention privacy-related thoughts in the decision rationale than participants who did not see a privacy notice (7.2%). A chi-square test shows this difference to be significant; \(\chi^2 = 93.75; p < .001\).

*Consumer Trust.* A similar pattern was observed for consumer trust. Specifically, purchase intent was lower among participants who saw a privacy notice, whether before, after, or both before and after the product features \((M_{\text{Before}} = 30.97 \text{ vs. } M_{\text{After}} = 36.33 \text{ vs. } M_{\text{Both}} = 33.93)\) than among those who did not see a privacy notice at all \((M_{\text{Absent}} = 47.42)\). An ANOVA shows this difference to be significant; \(F(3,763) = 10.00; p < .001; \eta^2_p = .04\). To determine if trust mediated the effect of the privacy notice on consumers’ interest in purchasing the product, we conducted a bias-corrected mediation analysis using PROCESS Model 4 (Hayes 2012). The mean indirect effect was negative \((a \times b = -9.20)\) with a 95% confidence interval excluding zero (-12.71 to -5.73), indicating significant mediation.
Willingness to Pay. A similar pattern was observed for willingness to pay (WTP). Specifically, WTP was lower among participants who saw a privacy notice, whether before, after, or both before and after the product features (Median\textsubscript{Before} = $500; M = $1,630; SD = $2,574; N = 180; vs. Median\textsubscript{After} = $800; M = $2,104; SD = $4,428; N = 187; vs. Median\textsubscript{Both} = $1,000; M = $2,126; SD = $3,144; N = 190) than among those who did not see a privacy notice at all (Median\textsubscript{Absent} = $1,500; M = $2,518; SD = $4,521; N = 188). This difference was not statistically significant; $F(3,741) = 1.71; p = .163; \eta^2 = .01$, but after removing outliers that were more than two standard deviations above the mean in each condition, this effect also became significant; $F(3,718) = 3.79; p = .01; \eta^2 = .02$.

Estimated Retail Price. Importantly, our manipulation did not affect expected retail prices. Expected retail price did not differ whether participants saw a privacy notice before, after, both before and after the product features (Median\textsubscript{Before} = $2,575; M = $3,786; SD = $3,225; N = 185; vs. Median\textsubscript{After} = $3,001; M = $3,755; SD = $3,066; N = 192; vs. Median\textsubscript{Both} = $3,381; M = $4,173; SD = $3,147; N = 195) or not at all (Median\textsubscript{Absent} = $3,015; M = $3,769; SD = $2,873; N = 195); $F(3,763) = .84; p = .48; \eta^2 < .01$. Viewed in light of the significant difference on the other measures, this null result suggests that the presence or absence of a privacy notice selectively influences the extent to which an individual consumer personally desires a product, but not the consumer’s perception of the objective value of the product in the marketplace. Finally, we compared participants’ perceptions that the product would retail at a premium relative to their individual willingness to pay; by subtracting WTP from the expected retail price, we calculated a “retail premium” for each individual. This retail premium was significantly higher among participants who saw a privacy notice, whether before, after, or both before and after the product features (Median\textsubscript{Before} = $1,001; M = $2,066; SD = $2,943; N = 180;
vs. Median$_{after}$ = $1,008; M = $1,533; SD = $4,007; N = 187; vs. Median$_{both}$ = $1,100; M = $1,925; SD = $3,094; N = 190) than among those who did not see a privacy notice at all (Median$_{absent}$ = $860; M = $1,222; SD = $3,840; N = 188). In short, the privacy notice lowers consumers’ own willingness to pay for a product, but not their estimate of its retail value.
Study 5 Stimuli

*Separate Evaluation – Privacy Notice Absent*

Suppose you need to buy some new clothes for an upcoming event and find some items you like on the website of an online retailer that you weren’t previously familiar with.

*Separate Evaluation – Privacy Notice Present*

Suppose you need to buy some new clothes for an upcoming event and find some items you like on the website of an online retailer that you weren’t previously familiar with.

Before proceeding to checkout, you notice a privacy policy. Proceed to the next screen to view the privacy policy.

*Joint Evaluation*

Suppose you need to buy some new clothes for an upcoming event and find some items you like on the websites of two online retailers that you weren’t previously familiar with.

Before proceeding to checkout, you notice a privacy policy on one site, but you can't find a privacy policy on the other site. Proceed to the next screen to view the privacy policy of the site that has one.
Privacy Policy

Categories of Information We Collect
We collect personal information when communicating or interacting with you through our website or family of companies. Personal Information is any information that we can use to identify, locate, or contact you. Some examples of Personal Information we collect include:
- precise location information if you provide it to us to (e.g., to show you the store nearest you)
- general location information from your browser or device (which we use for internal purposes, such as foot traffic analysis)
- contact information (e.g., name, email, phone, address) when you place an order
- financial information (e.g., credit or debit card number) when you make a purchase
- product preferences (e.g., when you browse our website, create a Wish List, complete Product Reviews, place an order, or make a return)
- physical characteristics (e.g., based on clothing size or when you are recorded by in-store cameras used for safety, security and operational purposes, such as to measure traffic patterns in our stores)

We may also collect personal information about you from other third parties, such as demographic firms, to make our future service and marketing efforts more efficient and personalized for you. We may combine all information we collect and we may disclose this information within our corporate family of companies or our service providers. When you visit our websites or other online services we may also gather certain information automatically and store it in log files. This information may include Internet Protocol (IP) addresses or other device identifiers, browser information, Internet Service Provider (ISP), operating system, location, date/time stamp and clickstream data.

Do We Share Your Information?
The information gathered may be shared with our family of companies. We also share the information with third parties, including responsible companies with which we have a relationship. We may share your personal information with unrelated outside companies so that they can directly market their products or services to you if we feel that a company offers products or services that we believe may be of interest.

Data Processing and Storage
We and our third party service providers may process or store your personal information outside of the United States. In accordance with the laws of those countries, in certain circumstances your personal information may be accessible by foreign law enforcement, regulatory bodies or other authorities.
Study 6 Stimuli

[Similar to Study 2, but the Realistic Privacy Notice was replaced by the Extra-Assuring Privacy Notice shown below and the Unseen Condition was added]

<table>
<thead>
<tr>
<th>Privacy Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Categories of Information We Protect</strong></td>
</tr>
<tr>
<td>We protect personal information when communicating or interacting with you through our website or family of companies. Personal information is any information that we can use to identify, locate, or contact you. Some examples of Personal Information we protect include:</td>
</tr>
<tr>
<td>- precise location information if you provide it to us (e.g., to show you the store nearest you)</td>
</tr>
<tr>
<td>- general location information from your browser or device (which we use for internal purposes, such as foot traffic analysis)</td>
</tr>
<tr>
<td>- contact information (e.g., name, email, phone, address) when you place an order</td>
</tr>
<tr>
<td>- financial information (e.g., credit or debit card number) when you make a purchase</td>
</tr>
<tr>
<td>- product preferences (e.g., when you browse our website, create a Wish List, complete Product Reviews, place an order, or make a return)</td>
</tr>
<tr>
<td>- Physical characteristics (e.g., based on clothing size or when you are recorded by in-store cameras used for safety, security and operational purposes, such as to measure traffic patterns in our stores)</td>
</tr>
<tr>
<td>We also protect personal information about you that we get from third parties, such as demographic firms, to make our future service and marketing efforts more efficient and personalized for you. We may disclose this information within our corporate family of companies or our service providers. When you visit our websites or other online services we may also gather certain information automatically and store it in log files. This information may include Internet Protocol (IP) addresses or other device identifiers, browser information, Internet Service Provider (ISP), operating system, location, date/time stamp, and clickstream data.</td>
</tr>
<tr>
<td><strong>Do We Share Your Information?</strong></td>
</tr>
<tr>
<td>The information gathered may be shared with our protected family of companies. We also share the information with third parties, including responsible companies with which we have a relationship. We may share your personal information with companies so that they may directly market their products or services to you if we feel that a company offers products or services that we believe may be of interest.</td>
</tr>
<tr>
<td><strong>Data Processing and Storage</strong></td>
</tr>
<tr>
<td>We and our trusted third party service providers may process or store your personal information outside of the United States. In accordance with the laws of those countries, in certain circumstances your personal information may be accessible by foreign law enforcement, regulatory bodies or other authorities.</td>
</tr>
</tbody>
</table>