Dec 12th, 12:00 AM

Using Active Privacy Transparency to Mitigate the Tension Between Data Access and Consumer Privacy

da ma
School of Management, mada_123@zju.edu.cn

Matthew J. Hashim
Eller College of Management, mhashim@arizona.edu

Qiuzhen Wang
School of Management , Zhejiang University, wqz@zju.edu.cn

Using Active Privacy Transparency to Mitigate the Tension Between Data Access and Consumer Privacy

Completed Research Paper

Da Ma
School of Management, Zhejiang University
Hangzhou, China
Mada_123@zju.edu.cn

Matthew J. Hashim
Eller College of Management, University of Arizona
Tucson, Arizona, USA
mhashim@arizona.edu

Qiuzhen Wang[1]
School of Management, Zhejiang University
Hangzhou, China
wqz@zju.edu.cn

Abstract

Recently, news exposure about privacy practices has brought substantial negative effects on companies' reputation and trust, which, in essence, reflects the escalating tension between data access and privacy protection that companies are currently facing. Accordingly, we design an active privacy transparency measure and implement it on our self-developed app. Through a two-task experiment, we simultaneously explore the profound and immediate effects of privacy transparency on firms and the underlying mechanisms. Results from our analyses show that active privacy transparency significantly mitigates users perceived psychological contract violations, which in turn helps companies prevent negative word-of-mouth and loss of trust. Moreover, it also ensures companies' immediate access to user data, and the moderating role of privacy literacy provides an explanation for this insignificant effect and previous inconsistent findings. More interestingly, we find that active privacy transparency might better elicit users' actual privacy preferences and help companies identify their targeted users.

Keywords: Active privacy transparency, data access, privacy protection, psychological contract violation, privacy literacy

Introduction

The free processing of users' data is considered an essential driver for firms' development and innovation in the age of the digital economy (Godinho de Matos et al. 2021). However, recent high-profile privacy news suggests that tensions dramatically arise between firms and consumers once a company's privacy practices are exposed by third parties.[2,3] It should be noted that the exposed news is not data breach, but rather firms' actual data handlings that comply with privacy regulations but might be less realized by users previously,

[1] Corresponding Author

[2]Please see https://www.chinadaily.com.cn/a/202110/14/WS61676ad5a310cdd39bc6ec27.html.
[3] Please see https://www.protocol.com/china/china-apps-surveillance-wechat.

such as the specific how users' personal data are collected and used by firms. Consequently, these privacy-related news brought substantial negative effects on companies, such as overwhelming negative word of mouth (NWOM), trust decline, and even drops in stock price (Martin et al. 2017; Mohammed 2022). Word-of-mouth and trust are the two core keys to building a friendly relationship between firms and users, which is crucial to the long-term success of businesses (Reichheld et al. 2000; Selnes 1998). Against this backdrop, companies must take user privacy protections into account by taking steps to prevent negative outcomes triggered by third-party exposure of privacy practices.

Firms that are not transparent about privacy practices proactively can be seen by consumers as party to a psychological contract violation (PCV). PCV is conceptualized as users' perception of being treated wrongly by services providers regarding the contractual obligations, which mainly occur due to two causes: companies' reneging because of opportunism and incongruence because of different understandings about obligations between buyer and seller (Morrison et al. 1997; Pavlou et al. 2005). PCV is especially effective at explaining the decrease in trust and word-of-mouth in e-marketplace (Chen et al. 2021; Rousseau 1989; Wang et al. 2018). In the context of privacy, with the disruptive development of information technology, information privacy has become a question with high complexity and uncertainty (Al-Natour et al. 2020). There exists serious information asymmetry between users and service providers (Acquisti et al. 2017; Acquisti et al. 2020); for providers, the collection and use of user information is par for the course, and most mainstream apps operate in a similar way; however, these privacy practices may be different from users' expectations, leading to PCV for consumers when privacy-related news is exposed by third parties. This brings us to argue that proactively providing privacy transparency in advance may be a potential way to prevent the negative impacts of privacy-related news.

Recent changes in privacy policies, such as the General Data Protection Regulation (GDPR)[4] and the Personal Information Protection Law (PIPL)[5], have put more attention and placed sweeping new requirements on privacy transparency (Tikkinen-Piri et al. 2018). However, these requirements remain at the legal norm level and do not provide explicit guidelines on how to establish privacy transparency (Betzing et al. 2020). In practice, privacy transparency information is generally hidden in firms' privacy policies as service providers always use this way to deal with the new laws and regulations. Such a hidden approach is called *passive* privacy transparency (Liu et al. 2022; Solove 2013), which is far from ideal in eliminating information asymmetry and protecting user privacy (Schaub et al. 2015). We focus on and design an *active* privacy transparency measure from the perspective of user privacy protection. Our active approach aims to proactively inform users about privacy practices and provide them with direct choices and real control of their information, thereby addressing the limitations of passive privacy transparency.

As the saying goes, "a slight move in one part may affect the whole situation." How privacy transparency will influence organizations' multiple and even competing privacy needs, the most representative one is the conflict between the long-term privacy protection-related reputation and the current information access, which is a primary obstacle for businesses to implement active privacy transparency. However, prior research only focuses on one side of the coin, while the systemic effect of privacy transparency is lacking (Gerlach et al. 2019). Moreover, the extant findings on privacy transparency impact are highly inconsistent. Some studies suggest that privacy transparency will have chilling effects (John et al. 2011; Keith et al. 2016; Kim et al. 2019; Zarsky 2016); some studies argue that transparency information is beneficial for trust-building and reducing vulnerability, and thus plays a promotional role (Aguirre et al. 2015; Godinho de Matos et al. 2021; Martin et al. 2017; Wang et al. 2018); and others surprisingly found that increased transparency features do not significantly alter individuals' privacy attitudes and behaviors, and the underlying reasons remain unclear and confusing (Karwatzki et al. 2017; Strycharz et al. 2021).

Given the privacy dilemma companies face in practice and the policy-practice gap in privacy transparency, this study aims to systematically investigate the immediate and profound effects of active privacy transparency. In this study, we define immediate effects as when users' grant privacy permission, a decision that usually needs to be made at that immediate moment. We define profound effects as potential impacts on companies' trust and WOM associated with privacy protection. In comparison to data sharing, changes

[4] Please see https://gdpr-info.eu/.

[5] Please see https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/.

in WOM and trust in a company may occur in the future, and both of them are important to businesses' long-term success, hence profound effects. Taken together, we aim to shed light on the following research questions: 1) Does active privacy transparency effectively prevent harmful effects such as negative word of mouth and trust decline introduced by privacy-related news? 2) Will this positive effect come at the expense of companies' ability to use consumer data? 3) What are the mechanisms underlying these impacts of active privacy transparency?

Theoretical Background and Hypotheses Development

Privacy Transparency

Issues around privacy transparency are considered critical by researchers and policymakers (Betzing et al. 2020; Fast 2019). Privacy transparency refers to the extent to which service providers inform users about firms' data handling practices (Karwatzki et al. 2017). It has been further explained as multiple dimensions, including clearly stating what personal information will be collected, for what purpose the acquired information will be used, and how the data will be processed and shared (Betzing et al. 2020; Godinho de Matos et al. 2021). The specific dimensions and content may vary across studies, but the essence is the same, that is aiming to empower users to make well-informed and self-interested privacy decisions (Tsai et al. 2011). In practice, however, the situation is totally different. How to establish and display privacy transparency is still largely at the discretion of companies (Betzing et al. 2020), thus it is not surprising that our investigation of mainstream apps shows that most of the transparency information can only be found in apps privacy policies. This kind of privacy transparency is used in many cases by companies to passively respond to privacy regulations (Liu et al. 2022), and we call it "passive privacy transparency". Substantial studies have found that such passive privacy transparency is neither usable nor useful in protecting user privacy and eliminating information asymmetry (Schaub et al. 2015). Changes in privacy regulations, from the basic informed consent mechanism to the transparency enhanced consent represented by GDPR and PIPL, indicate a trend toward more specific and stricter requirements for privacy transparency. Therefore, this paper focuses on active privacy transparency relative to passive privacy transparency. We design an active privacy transparency measure in the context of mobile applications, which is mandatory reading and give individuals direct control over their personal information, compensating for the limitations of passive privacy transparency.

Scholars have conducted useful explorations on privacy transparency; however, the extant literature is still ambiguous, different types of privacy transparency are not distinguished, and findings on the impact of privacy transparency are highly inconsistent. Some studies found that the impacts of privacy transparency are positive and promotional, such as more data allowance, higher personalized advertisements click intention, and even a smaller drop in stock price after a data breach (Aguirre et al. 2015; Godinho de Matos et al. 2021; Martin et al. 2017; Morey et al. 2015). However, some studies found contrary effects, for example, privacy transparency may cause people to tend to deny privacy permission requests, decrease the effectiveness of targeted advertisements, and even hinder the innovation of the whole society (John et al. 2011; Keith et al. 2016; Kim et al. 2019; Samat et al. 2017; Zarsky 2016). Some recent research has even found that the privacy transparency feature does not significantly shape users' privacy decision-making (Betzing et al. 2020; Karwatzki et al. 2017; Strycharz et al. 2021). Although scholars tried to put forward some speculations for these unexpected findings, the underlying reasons remain unclear and confusing. Additionally, existing literature only focuses on the impact of privacy transparency in a specific aspect. Organizations have multiple privacy needs that are often even competing, such as the current data collection or long-term privacy protection-related reputation. Privacy transparency may play different roles in fulfilling companies' competing demands. However, this systemic and multidimensional effect of privacy transparency is lacking in prior research. This gap is notable because it is what businesses really care about and struggle with in designing and implementing privacy transparency. Xu et al. (2021) proposed that the theory-practice gap—privacy research does not resonate well with companies' practice—is a salient conundrum in the state of privacy research. Gerlach et al. (2019) suggested that a crucial reason why extant studies cannot be transferred to managerial privacy practice is that they only reveal one side of the coin. These gaps call for research to further investigate the joint impacts of active privacy transparency on companies' immediate and profound privacy needs and to explain the mechanisms underlying these effects.

Profound Effects of Active Privacy Transparency

Forbes Insight Report[6] shows that issues related to information privacy and security have the potential to do the most damage to companies' reputations and trust. Previous studies have shown that when companies' actual privacy practices are exposed by social media, it usually causes considerable negative word-of-mouth for businesses and leads to a significant drop in user trust (Martin et al. 2017; Mohammed 2022). According to relationship marketing theory, word-of-mouth and trust are two core elements for companies to build long-term relationships with users (Reichheld et al. 2000; Selnes 1998). Once they are damaged, the negative impacts could last into the future. Therefore, in this paper, we focus on the NWOM and trust decline and use them as proxies to characterize so-called profound effects.

NWOM refers to individuals spreading negative or even adverse feedback and reviews to their friends, relatives, and strangers, which is often seen as an active user reaction to a bad experience (Balaji et al. 2016; Son et al. 2008). Substantial studies have focused on the motivational factors related to NWOM and found that various elements, such as personal characteristics, emotions, and goals are related to engaging in NWOM (Chang et al. 2015; Nguyen et al. 2021; Wetzer et al. 2007). Essentially, the influence of these factors overwhelmingly reflects that the unsatisfactory imbalance between expectations and perceptions plays a key explaining mechanism for user-generated NWOM (Buttle 1998; Williams et al. 2014). This inconsistency between what people expect and actually perceived to be treated is precisely PCV.

Psychological contracts are quite widespread in nature; when one party believes that another party should perform certain behaviors, a psychological contract is established (Rousseau 1989). PCV is thus defined as users' perception that they are not being treated as contracted (Chen et al. 2021). PCV theory was initially widely used in the field of organizational behavior, and academics and practitioners alike have suggested that users perceived PCV can effectively explain or predict various negative phenomena, such as the decrease in trust, job satisfaction, and generation of NWOM in the context of employee-employer relationship building (Chih et al. 2017; Robinson et al. 1994). More recently, studies have further validated the central role of PCV in a broader online marketplace (Chen et al. 2021; Wang et al. 2019), and extant literature consistently suggests that PCV may arise from two causes: incongruence and reneging (Morrison et al. 1997; Pavlou et al. 2005).

Incongruence occurs when two parties have different understandings of the psychological contract (Morrison et al. 1997). In the context of our research, incongruence largely stems from the fact that there exists significant information asymmetry between users and firms in current privacy practices (Acquisti et al. 2017; Acquisti et al. 2020). As data practice becomes more complex and users lack expertise, the beliefs that users hold about how personal information is processed by service providers may differ from what they actually do. Therefore, when users know corporate actual practices from third-party news exposures, even if they are in compliance with privacy regulations, a high level of incongruence occurs. After implementing active privacy transparency, businesses' privacy practices, such as what information will be collected and how these data will be handled, will be clearly notified and mandatory to be read by users in advance. This can clarify and update users' privacy understanding and knowledge and thus reduce privacy uncertainty and incongruence (Al-Natour et al. 2020; Gerlach et al. 2019). Therefore, under the condition of active privacy transparency, users should have lower perceived PCV caused by incongruence. Moreover, previous studies have generally found a significant effect or explanation of such PCV on users' NWOM in both online and offline scenarios. For example, Mehmood et al. (2018) found that in the field of online retailing, consumers' NWOM for service failure results from PCV. In face-to-face sales scenarios, the restaurant remedies would be effective in reducing the likelihood of consumers engaging in NWOM if these measures could mitigate PCV (Chen et al. 2021; Chih et al. 2017). Therefore, we contend that when users read news about a company's privacy practices, active privacy transparency that reduces PCV by resolving privacy incongruence in advance will further prevent users' NWOM, and we posit the following hypothesis.

Hypothesis 1. Active privacy transparency has a negative influence on users' perceived PCV, which, in turn, leads to a decrease in users' negative word-of-mouth triggered by privacy news.

Another primary cause of PCV is reneging, which refers to one party deliberately failing to meet the obligations because it is unwilling to do so (Morrison et al. 1997). In current privacy practices, the

[6] Please see https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html

transparency information is always passive, and users are unaware of companies' measures and efforts at transparency (Liu et al. 2022; Schaub et al. 2015). When third parties expose companies' actual privacy processes, it will make users believe that service providers are intentionally hiding their privacy practices due to opportunism, and thus reneging arises. Active privacy transparency allows companies to proactively disclose their information practices themselves before users make privacy decisions (Betzing et al. 2020; Godinho de Matos et al. 2021). Just like "leniency for those who confess," no matter what the transparency content is, this action could be enough to demonstrate companies' motivation and sincerity in privacy transparency, thereby reducing users' perceived PCV caused by reneging.

Additionally, trust is a core construct and a great deal of literature shows that trust is one of the most salient beliefs in privacy-related contexts (Malhotra et al. 2004). In this paper, we conceptualize trust in a broad sense as a general belief or expectation that the trusted party will fulfill commitments and not behave opportunistically (Gefen et al. 2003). Given that the trust destruction associated with increasing privacy news would be fatal to businesses' long-term success, this study focuses on how to prevent or mitigate trust decline. Unlike incongruence, a typical feature of reneging is knowingly failing to fulfill the contract (Morrison et al. 1997), and in this case, individuals tend to make malicious attributions, which has been widely found to well explain trust decline in previous studies (Robinson 1996). For example, in the workplace, Niehoff et al. (2001) revealed that reducing PCV is critical to rebuilding trust with employees. Piccoli et al. (2003) found that trust decline in virtual teams is rooted in PCV caused by reneging. Wang et al. (2019) showed that for a biased RA, discoursing sponsorship could reduce PCV, which in turn leads to higher perceived trust. Additionally, Wang et al. (2018) shows that remedial measures can only mitigate, not wholly eliminate or reverse, the original PCV and negative outcome to a certain extent. Similarly, in our study, privacy news exposed by third parties inherently leads to a drop in trust. However, we argue that the decrease in trust will be mitigated after providing active privacy transparency information, since proactive and candid transparency reduce PCV derived by reneging. Therefore, we propose the following hypothesis:

Hypothesis 2. Active privacy transparency has a negative influence on users' perceived PCV, which, in turn, leads to a lower trust decline in response to privacy news.

Immediate Effects of Active Privacy Transparency

Regarding immediate effects, the most direct and crucial to businesses is how active privacy transparency will influence user privacy permission granting (Gerlach et al. 2019). However, this issue is still ambiguous in extant literature and open to debate. One stream of work suggests that privacy transparency could have a positive effect on user information sharing. For example, Morey et al. (2015) proposed that privacy transparency is a tactic to help companies earn ongoing data access from users; Godinho de Matos et al. (2021) found a facilitating effect of privacy transparency on users' data allowances. Such studies interpret privacy transparency as a signal of trust. However, some studies hold a different view, arguing that privacy transparency is a risk signal. When providing transparency information proactively, privacy concerns become more explicit and salient, and thus users tend to deny privacy permission requests and reduce information disclosure (John et al. 2011; Keith et al. 2016). In addition, some studies found that privacy transparency does not have a significant impact on user information sharing, which is speculated to be a joint effect of risk and trust mechanisms (Karwatzki et al. 2017).

These inconsistent findings are essentially reflecting a debate about whether privacy transparency is a privacy risk or a trust signal. In practice, the information that companies are most worried about and unwilling to let users know is usually those privacy practices with high privacy sensitivity and low user acceptability. It is also the privacy news exposing these privacy practices that make companies the target of public criticism. That is, the transparency information that evokes a high perception of privacy risk is the point. Moreover, according to the well-known negativity bias, even if both the risk and trust features of privacy transparency are present, people are instinctively more sensitive to privacy risk, which is more influential in users' privacy decision-making (Baumeister et al. 2001; Kim et al. 2019). Consequently, we posit the following hypothesis on the immediate effects of active privacy transparency.

Hypothesis 3. Active privacy transparency increases users' perception of privacy risk, which, in turn, leads them to be less likely to grant privacy permission.

Experiment

To examine the proposed hypotheses, we first designed an active privacy transparency measure. Then, we conducted a two-task controlled laboratory experiment: Task 1 is a privacy permission setting task, where we manipulate the presence or absence of active transparency information to investigate its immediate effect; In task 2, we simulate third-party privacy news exposure to explore the profound effects of privacy transparency. The manipulation of privacy transparency and experimental tasks were implemented through our own experimental mobile application which allows us to also capture users' actual behaviors.

Pre-test

Prior to the formal experiment, we recruited 77 participants for a pre-test to select content for the manipulation of privacy transparency used in the following experiment.

Transparency Content Generation. M-commerce has become a vast market with a broad user base, and personalized recommendation services have attracted growing attention from privacy researchers due to their high reliance on personal information. Therefore, we used the privacy setting of m-commerce's personalized recommendation as our experimental scenario. We first summarized the information privacy practices underlying personalized recommendation functions from the privacy policies of the Top 5 m-commerce Apps in China.[7] Then, following the definitions of privacy transparency in prior literature (Godinho de Matos et al. 2021; Karwatzki et al. 2017), we divided the obtained privacy practices into five dimensions: the scope of data collection, the purpose for data using, and how the data will be processed, shared and protected. Finally, we generated a selection set with five items of privacy transparency content.

Transparency Content Selection. Privacy news with strong negative outcomes is often associated with privacy practices that have low user acceptability (Kim et al. 2019). Acceptability refers to the extent to how well a measure is received by the target population (Ayala et al. 2011), and here we use it to reflect users' opinions about how companies handle their personal information. These low-acceptance privacy practices are also what companies worry about most in implementing active privacy transparency. Therefore, participants in the pre-test were asked to read each privacy transparency item in the selection set and rate their acceptability using a seven-point scale from 1 (Entirely Unacceptable) to 7 (Entirely Acceptable). The item with the lowest score will be selected as the stimulus for the formal experiment.

Analysis and Results. We performed a Friedman test and found significant differences in participants' acceptability of the five privacy transparency dimensions ($\chi^2(4, 77) = 160.33$, $p < 0.001$). To compare dimensions to each other, we conducted post-hoc full pairwise comparisons and treated each dimension as the reference class in separate analyses. The results indicated that participants have the lowest acceptability of transparency information about data collection than any other four items (see Table 1). Therefore, the item of data collection, which data will be collected under the personalized recommendation service, will be used as privacy transparency text in the following experiment.

		Test Statistic of Pairwise Comparison			
	Average Rank	Collection	Processing	Purpose	Sharing
Collection	1.42	-	-	-	-
Processing	2.66	-1.234***	-	-	-
Purpose	3.21	-1.792***	-0.558	-	-
Sharing	3.42	-2.000***	-0.766*	-0.208	-
Protection	4.29	-2.864***	-1.630***	-1.071***	-0.864**
Friedman χ^2	160.326***				

Table 1. Full Pairwise Comparisons on the Five Privacy Transparency Dimensions

Note. *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

[7] Please see http://enet.com.cn/article/2022/0118/A202201181266746.html.

Experimental Design

The investigation of some popular m-commerce Apps shows that today's personalized recommendation feature is often enabled by default, and its transparency information is passive and hidden in Apps' privacy policies (Betzing et al. 2020; Schaub et al. 2015). Unlike current privacy practices, we designed an active privacy transparency measure, as shown in Figure 1, Condition 2. Specifically, we first changed the personalized recommendation from a default function to opt-in permission presented in the privacy settings popup. Then, we improved the traditional privacy setting process by inserting a new interface to explain the relevant privacy transparency information before users' final decision. The design differs from the current passive privacy transparency in three ways: (1) In the first interface, there is only one option of "click to read the transparency information", which solves the lack of knowledge problem caused by users not reading; (2) The transparency content is directly linked to permission decision-making, giving users actual control on their privacy; (3) The design informs users of privacy transparency information in a proactive way, rather than passively abiding by privacy regulations. In this study, we employed a between-subjects experimental design, where the control group was not given transparency information, and the experimental group adopted our new design of active privacy transparency (see Figure 1).

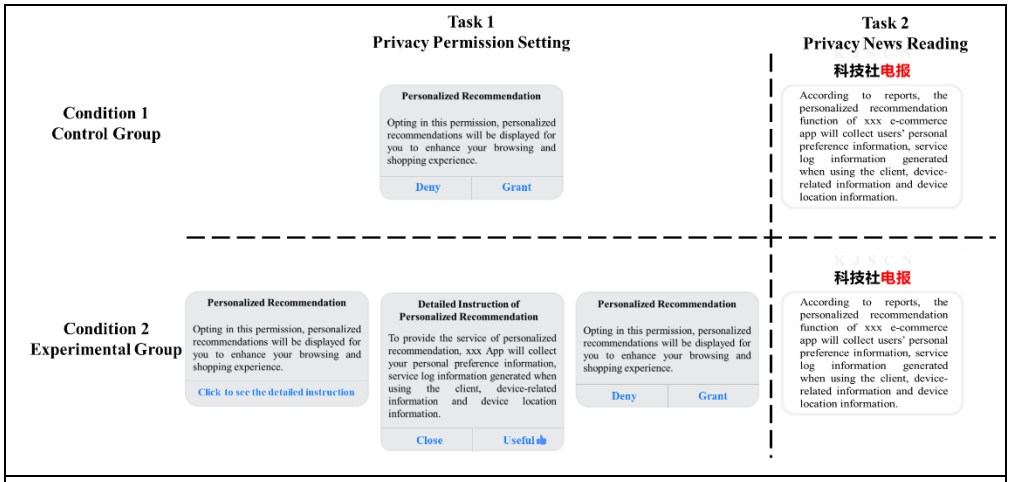

Figure 1. Experimental Flow

Participants and Procedure

We recruited participants from a large public university in China. The participants were required to have at least two years of experience using mobile apps, and those who took part in the pre-test were excluded. To conceal the real research purpose and make the scenario more realistic, we informed participants that they were invited to take part in an internal test of a company's new online shopping app. The subjects who completed the test would be paid 10 RMB. A total of 80 qualified participants were recruited to ensure a sufficient statistical power of 0.90 (1-β) for detecting a large effect (f = 0.4). Due to failing attention checks, five responses were eliminated and left 75 valid observations (54 females, average age =21.88).

Figure 1 illustrates the experimental flow. Upon arrival, participants were first informed of the procedure of our study, and they need to sign a consent form. Next, participants were randomly assigned to the two experimental conditions and finished two tasks in sequence. In task 1, participants installed the beta m-commerce app on their mobile phones and were told that they could browse and use this app freely just as they would in any other app. Soon after opening the app, a permission setting notification for the personalized recommendation popped up. This procedure is in line with actual mobile app use, where first-time users will be immediately asked for privacy permission settings. Participants in the control group just needed to decide whether to grant or deny the personalized recommendation permission request as usual, while people in the experimental group were required to read the privacy transparency information and evaluate whether the content was useful before deciding to enable or close this privacy permission. After finishing the permission setting, participants in two groups were asked to fill out a post-task questionnaire. Then, in task 2, we present them with a news report regarding the data handling behind the beta app's

personalized recommendation (same content as transparency in task 1), which is used to simulate companies' privacy practices exposed by third-party media. All participants were required to read the same news and complete the task 2 post-task questionnaire. After finishing all tasks, we explained to our participants the purpose of this study and gave them opportunities to opt-out. All the participants confirmed their participation.

Measurement

Our experimental measurements consist of two parts. One part is users' actual behavioral data recorded by our self-developed app. During the experiment, the app automatically recorded participants' actual decisions on the privacy permission of personalized recommendation (grant versus deny). For the group with active privacy transparency, we additionally collected users' reading time and choices of transparency information (useful versus close).

The other part is self-reported data collected by post-task questionnaires. All measurement items were adapted from previous validated studies (see Table 2). In the task 1 questionnaire, we first asked participants to recall their choices in the experiment, and this was used as an attention check question. Then, we measured users' perceived consistency between experimental instructions and their original knowledge (Kim et al. 2019), perceived privacy risk when setting the privacy permission (Libaque-Sáenz et al. 2021), and trust in the app (Liu et al. 2022). Last, we included questions "Is the app's description of information processing transparent, clear, and straightforward" to check the manipulation of privacy transparency (Martin et al. 2017; Wang et al. 2018). In the task 2 questionnaire, we measured participants' negative word of mouth (Martin et al. 2017) and perceptions of psychological contract violations (Pavlou et al. 2005). In addition, we asked users' trust in the app again to reflect changes in trust. Finally, respondents' demographic information, including gender, age, and privacy experience, was asked.

Constructs Measures [Scale: from 1 "Strongly disagree" to 7 "Strongly agree"]		
Constructs	**Measurement items**	**Source**
Perceived Consistency	The description of the privacy permission in this app is consistent with my original knowledge.	(Kim et al. 2019)
Perceived Privacy Risk (PR)	When setting the privacy permission in this app, I feel that using this service would be risky.	(Libaque-Sáenz et al. 2020)
	… I feel that using this service would be insecure.	
	… I feel that using this service may lead to high privacy concerns.	
	… I feel that using this service may involve a high potential for privacy loss.	
Trust	In general, I feel that this app is reliable.	(Liu et al. 2022)
	In general, I feel that this app is trustworthy.	
	In general, I would characterize this app as honest.	
Negative Word of Mouth (NWOM)	Following this experience with the app, I would likely give a negative review to this app	(Martin et al. 2017)
	… I would likely bad-mouth the app to my friends, relatives, or acquaintances.	
	… I would likely advise other people not to use this app.	
	… I would likely spread negative word of mouth about this app.	
Psychological contract violations (PCV)	After reading the news, I feel that this app failed to meet its obligations to inform me about privacy during our interactions.	(Wang et al. 2018)
	… I feel that this app did a poor job of meeting its obligation to inform me about privacy during our interactions.	
	… I feel that this app did not fulfill the most important privacy informing obligation to me during our interactions.	

Table 2. Post-task Survey Instrument

Data Analyses and Results

Manipulation Checks

We first conducted an analysis of variance (ANOVA) to check the manipulation of privacy transparency. The results showed that the permission request presented with detailed collection information (in experimental group) was perceived to have significantly higher privacy transparency (mean = 3.45) than that without such information (in control group) (mean = 2.83, $F(1,73) = 4.269$, $p < 0.05$). Thus, our manipulation of privacy transparency was successful. In addition, the Mann-Whitney and ANOVA tests revealed that participants assigned to the two experimental conditions did not differ significantly in terms of gender ratio, age, and previous privacy experience, suggesting that the sample was well balanced across the baseline characteristics, and the random assignment appeared to be effective.

Measurement Validation

We conducted exploratory and confirmatory factor analyses to examine the reliability and validity of the measurement scales. As shown in Table 3, the Cronbach's α and composite reliability (CR) of all constructs were above the minimum critical value of 0.7 (Hair Jr. et al. 2017), indicating that the scales of our constructs had good internal consistency and reliability. All the intercorrelations are smaller than 0.6, and the square root of the average variance extracted (AVE) for each construct was larger than its correlations with any other constructs. The results indicate strong evidence of convergent and discriminant validities.

Variable	Cronbach's α	CR	AVE	Correlations				
				Privacy Risk	Trust 1	PCV	NWOM	Trust 2
Privacy Risk	0.946	0.961	0.860	0.927[a]				
Trust 1	0.946	0.965	0.901	-0.148	0.949			
PCV	0.931	0.956	0.878	0.336	-0.181	0.937		
NWOM	0.911	0.938	0.791	0.380	-0.123	0.353	0.889	
Trust 2	0.929	0.939	0.877	-0.309	0.466	-0.594	-0.259	0.936

Table 3. Construct Reliability and Validity

[a]Diagonal elements are square roots of AVEs, and off-diagonal elements are interconstruct correlations.

Hypotheses Testing

Profound Effects

We first analyzed participants' responses in task 2 to answer the question: Is active privacy transparency a potential way to prevent companies from negative effects introduced by privacy-related news exposure?

We adopted a linear regression model to examine the main effects of privacy transparency with NWOM and trust decline as dependent variables. We generated a new variable—"Trustdid", which equals to the trust measured in task 1 minus that in task 2, and used it to characterize the changes in users' trust. The variable *Transparency* is an indicator of the independent variable that takes the value of 1 if participants were assigned to the group with active privacy transparency information. The results in Table 4 indicated that privacy transparency has significant negative effects on NWOM (β = -0.762, p = 0.009) and Trustdid (β = 0.642, p = 0.018), and these effects remained consistent after considering control variables (gender, age, and previous privacy experience). In other words, providing transparency information proactively could effectively reduce negative word of mouth and mitigate trust decline when users read negative privacy news.

To further examine the underlying mechanism of the privacy transparency effects, we performed bootstrapping mediation tests following Hayes (2017) (PROCESS Model 4, bootstrapping samples = 5000), with privacy transparency as the independent variable, psychological contract violations as the mediator, and users' NWOM and Trustdid as the dependent variables, respectively. The results reported in Figure 2 revealed significant indirect effects of privacy transparency on NWOM (β = -0.25, SE=0.14, 95% CI = [-

0.58, -0.03]) and on Trustdid (β = -0.22, SE=0.12, 95% CI = [-0.47, -0.01]) through psychological contract violations. Meanwhile, the direct effects of privacy transparency became insignificant. Hence, the mitigation effects of privacy transparency on users' negative word of mouth and trust decline were fully mediated by their psychological contract violations. Therefore, H1 and H2 were supported.

Variables	NWOM		Trustdid	
	Model 1 without control variables	Model 2 with control variables	Model 3 without control variables	Model 4 with control variables
Transparency (0-absence, 1-present)	-0.762**(0.285)	-0.706* (0.270)	-0.642*(0.266)	-0.693** (0.254)
Age		-0.032 (0.045)		-0.013 (0.042)
Male		0.793**(0.301)		-0.464(0.283)
Experience		0.163(0.086)		-0.214**(0.081)
Constant	3.853*** (0.198)	3.618**(1.063)	1.402*** (0.184)	2.75**(1.002)
Observations	75	75	75	75

Table 4. Main Effects of Privacy Transparency on NWOM and Trust Decline

Note. *p < 0.05; **p < 0.01; ***p < 0.001

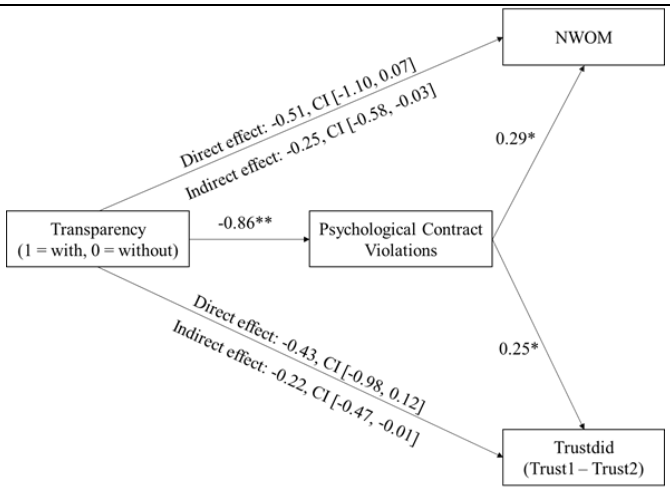

Figure 2. Mediation Effects of Psychological Contract Violations

Note. *p < 0.05; **p < 0.01; ***p < 0.001

Immediate Effects

Next, we analyzed participants' responses in the task 1 to answer whether the above positive profound effects of privacy transparency would accompany a decline in privacy permission granting.

We conducted a binary logistic regression to test the immediate effect of privacy transparency. Users' actual choice of the privacy permission in the first task was used as the dependent variable (code as 1 for granting this privacy permission and code as 0 if participant denied). Unlike the negative impact we hypothesized, the results in Table 5 showed an insignificant relationship between privacy transparency and permission granting (β = 0.474, p = 0.484). This suggests that whether or not to provide privacy transparency information to users proactively does not change their actual privacy permission granting behavior notably. Hence, H3 was not supported by the data.

Variables	Permission Granting (1=Grant, 0=Deny)	
	Model 1 without control variables	Model 2 with control variables
Transparency (0-absence, 1-present)	0.474(0.484)	0.431 (0.528)
Age		0.066 (0.086)
Male		-0.729 (0.626)
Experience		-0.520**(0.180)
Constant	-0.811* (0.347)	0.061 (1.989)
Observations	75	75

Table 5. Effects of Privacy Transparency on Privacy Permission Granting

Note. *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

Post Hoc Analysis

At face value, our study suggests that users' privacy permission granting behavior will not be affected by privacy transparency. However, the mechanisms underlying this null effect might be complex, and it is possible that there are effects that did not manifest in the analysis of the main factors. Therefore, we conducted several post hoc analyses to understand users' this privacy behavior further.

Deconstructing Users' Disclosure Decision

As introduced in the experimental procedure, we also recorded users' responses to the transparency content in the first task, including users' reading time and usefulness choice (useful versus close) in the transparency interface. According to this data, we were surprised to find that all participants who "grant" the privacy permission in the condition with privacy transparency were those who chose "useful" for transparency information, and they generally took a longer time to read the transparency content than "deny" or "close" users (see in Table 6). Intuitively, these results indicated that when providing privacy transparency in advance, individuals' privacy permission granting decisions tend to be made after deliberate thinking.

	Useful	Close	Total
Grant	15（RT=11.50）	0	15
Deny	4 (RT=9.45)	17（RT=10.31）	21
Total	19	17	36

Table 6. Summary of Participants' Choices in Transparency Condition

Additionally, we conducted a one-way analysis of variance (ANOVA) to compare the NWOM and Trustdid of participants granted privacy permission under different transparency conditions. The results revealed that, compared to the condition without privacy transparency, if participants grant privacy permission under the condition of transparency, then they would be less likely to reduce trust ($F = 9.60$, $p < 0.01$) and generate negative word of mouth ($F = 4.73$, $p < 0.05$) when reading negative privacy news. This further verified that although privacy transparency has no significant impact on users' permission granting, in the presence of transparency information, people tend to make well-informed and deliberative privacy choices.

The Role of Users' Prior Privacy Literacy

The essence of privacy transparency is to inform users about companies' privacy practices, and a hidden assumption of Hypothesis 3 is that users know little about what companies actually do with their personal information. But in reality, users have different levels of privacy literacy, and thus the privacy transparency information may be new knowledge to some users but known to others. Therefore, we speculate that a potential explanation for the insignificant impact of privacy transparency on users' permission granting

behavior is the differences in users' original privacy literacy, which has also been found in previous literature to be an important but easily overlooked individual characteristic in influencing user privacy decision-making (Bartsch et al. 2016; Brough et al. 2019).

Although we did not measure users' privacy literacy directly, we can derive it from the manipulation of privacy transparency and the measured users' perceived consistency (between experimental instructions and their original knowledge). The calculation rules are shown in Table 7. Specifically, for participants assigned to the transparency group, if their perceived consistency was above average, we labeled this subject as "high privacy literacy" with a value of 1; otherwise, it was "low privacy literacy" with a value of 0. The rules are reversed for individuals in the control group: we labeled them as "high privacy transparency" if their perceived consistency was below average.

Transparency (manipulate)	Consistency (measure)	Privacy literacy (calculus)
1	High (>mean)	High-1
1	Low (<mean)	Low-0
0	Low (<mean)	High-1
0	High (>mean)	Low-0

Table 7. Calculation Rules for Privacy Literacy

We conducted a moderation analysis following Hayes (2017) (PROCESS Model 1, bootstrapping samples = 5000), with privacy transparency as the independent variable, privacy literacy as the moderator, and users' actual choices of the privacy permission as the dependent variables. The results revealed a significant interaction between privacy transparency and users' privacy literacy (b = 3.39, SE = 1.42, p = 0.017). The simple effect analysis showed clearly that (see Figure 3), privacy transparency increased the likelihood of high privacy literacy users' permission granting (b = 1.78, SE = 0.86, p = 0.039), but for users with low privacy literacy, the effect was reversed but insignificant (b = -1.61, SE = 1.13, p = 0.16).

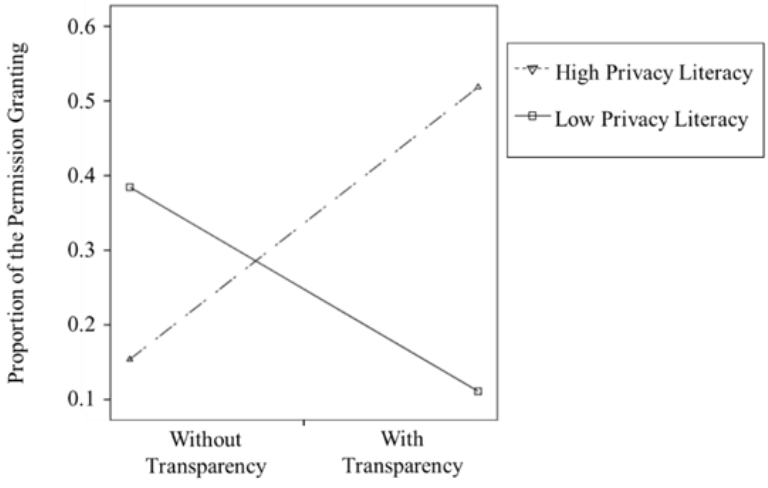

Figure 3. Moderating Effect of Privacy Literacy

Discussion and Conclusion

Research Summary and Key Findings

Addressing the escalating tension between data access and consumer privacy is a critical and urgent issue facing companies in the current era. Our study sought to provide insight into this question by designing a privacy-enhancing active privacy transparency measure and exploring its role in fulfilling companies' competing privacy needs. We conducted a two-task controlled laboratory experiment using the self-

developed app and yielded several important findings. First, results of the second task support the hypotheses drawn from the theoretical lens of PCV that active privacy transparency effectively mitigates users' perceived PCV, which in turn helps companies prevent the negative word-of-mouth and loss of trust resulting from third-parties exposure of companies' privacy practices. This is beneficial for companies to build a privacy-friendly relationship with users and earn long-term business success. Second, the first task results suggest that the profound positive effects of active privacy transparency do not come at the expense of an immediate reduction of data collection for a company. Users' privacy permission granting decision does not decrease significantly; more interestingly, we observe that peoples' granting decisions in transparency condition take a longer time to make and are accompanied by less NWOM. In other words, active privacy transparency not only retains companies' data access but also elicits deliberative permission granting choices from users. Third, the post hoc analyses demonstrate a significant moderating effect of privacy literacy, which provides a plausible explanation for the insignificant effect of active privacy transparency on user permission granting. Active privacy transparency significantly increases permission granting for users with high privacy literacy, but the effect is insignificant for low-privacy literacy users and even implies an opposite trend. The two different effects may cancel each other out, resulting in an insignificant aggregate impact.

Theoretical Contributions

Our study makes important contributions to the growing body of research regarding privacy transparency. First, we extend the existing literature by distinguishing two types of privacy transparency, active and passive. Recent changes in privacy regulations reflect the increasingly strengthened requirements for privacy transparency. However, due to the lack of guidelines on implementation and organizations' sophistication and motivation to obtain more data, transparency information is often hidden in companies' privacy policies in current privacy practices. That is, there is a gap between policy expectations and firm practices concerning privacy transparency. We differentiate between active and passive privacy transparency in terms of whether users are required to read the transparency information and act with direct and real control of their information. Accordingly, we design and implement an active privacy transparency on our self-developed app, which strengthens user privacy protection upon current privacy practices. We clarify the different types of privacy transparency, which helps avoid research confusion caused by definitions and scopes and provides a basis for the following research.

Second, to our knowledge, this study is the first to empirically examine the profound and immediate effects of privacy transparency simultaneously. Previous literature about privacy transparency has focused primarily on its effect on a particular behavior or in a certain aspect, such as information disclosure, service adoption, or privacy protection. However, as some more recent studies have called for, privacy issue in the realistic scenario is complex (Buckman et al. 2019), and the effect in one part alone does not represent the ultimate outcomes (Adjerid et al. 2019) and cannot resonate with managerial practices (Xu et al. 2021). Gerlach et al. (2019) interviews with practitioners also implied that some suggestions of privacy transparency are not being adopted by companies because they only underline one side of the coin. Our research fills this gap by exploring the impact of privacy transparency on the two competing privacy needs companies are concerned about most: long-term WOM and trust associated with privacy protection versus immediate data access, which also produces a more overarching insight into the role of privacy transparency.

Lastly, we provide an insightful explanation for the current inconsistent findings of privacy transparency. Prior research has mainly debated the trust or privacy risk mechanisms underlying privacy transparency, which has further led to two entirely opposite conclusions (Aguirre et al. 2015; Karwatzki et al. 2017; Kim et al. 2019; Martin et al. 2017). Our findings on the moderating role of privacy literacy offer a new insight: the impact of privacy transparency may vary depending on individuals' privacy literacy. Specifically, in our context, we found that for high privacy literacy users, privacy transparency enhances the likelihood of permission granting, but for low privacy literacy users, the effects of transparency on users' data allowance are insignificant and even presents an opposite trend in terms of the mean value. This finding contributes to the mechanism of privacy transparency from the perspective of user privacy characteristics and reveals the crucial role of privacy literacy.

Managerial Implications

The findings of this study also provide valuable managerial implications. From a firm perspective, we first suggest a feasible way for companies to balance the increasing tension between data access and consumer privacy. Our empirical study shows that implementing active privacy transparency could help companies build a good reputation for privacy protection and maintain a trusting relationship with users while also ensuring access to user data and digital innovation. Additionally, our results demonstrate that companies could implement targeted marketing strategies in conjunction with active privacy transparency. We observe that after providing active privacy transparency, participants typically spend more time and make full use of the transparency information in privacy granting decision-making, and they are less likely to generate NWOM and trust decline. In that case, active privacy transparency might better elicit users' actual privacy preferences and, in turn, help companies identify their targeted users. As a result, companies may tailor targeted marketing strategies based on users' privacy preferences. Lastly, our study recommends that firms could spend more money and effort on user privacy literacy education in the future. Our results indicate that individuals' privacy literacy plays a critical role in the effectiveness of active privacy transparency; for users with a high-level privacy literacy, active privacy transparency may even help companies earn expanded data access. Therefore, improving user privacy literacy in an understandable and acceptable way could be an issue that companies need to pay more attention to. From a policy perspective, our results call for fine-grained requirements for privacy transparency, moving from a legal norm level to more explicit established guidelines. In current privacy practice, the design and display of privacy transparency remains largely under the control of service providers, which is a major cause of passive privacy transparency. While our findings presented in this paper show that proactive and candid transparency enhances privacy protection and, at the same time, preserves companies' reputation and trust in privacy and allows companies to extract value from user data. As such, it creates a virtuous circle and is an important step in promoting a healthy and privacy-friendly environment.

Limitations and Future Research Directions

This research has three major limitations and provides some insights for future research. The first limitation is the sample size. In this manuscript, we recruited 157 subjects in total, including 77 in the pre-test and 80 in the formal experiment. Before experimenting, we calculated the required sample size with G*Power 3.1 and found that 80 participants are enough to ensure a sufficient statistical power of 0.90 (1-β) for detecting a large main effect (f = 0.4). However, this sample size may limit further analysis, such as the mediating effects and post-hoc analysis. Therefore, in a follow-up study we plan to expand the sample size to improve our findings. Second, participants' privacy literacy used in our study was calculated by the manipulation of active privacy transparency and the measurement of perceived consistency. According to the definition, this is one way in which users' privacy literacy can be captured in our research context (Brough et al. 2019; Trepte et al. 2015). Future research could employ other methods, such as direct measurement and manipulation, to further examine the role of users' privacy literacy from various aspects. Moreover, our findings on the moderating role of privacy literacy call for more research that focus on privacy literacy. Finally, our experiment only manipulated the collection dimension of privacy transparency based on the pre-test result regarding acceptability and is not exhaustive. This item was found to have the lowest acceptability, which is often the most worrisome component for companies implementing active privacy transparency. Future research could examine other dimensions and how to design the choice architecture of the active privacy transparency based on our research that may have different impacts on users' privacy decision-making (Acquisti et al. 2020; Adjerid et al. 2018).

Acknowledgements

This work was supported by the National Natural Science Foundation of China [grant number 72071177].

References

Acquisti, A., Adjerid, I., Balebako, R.*, et al.* 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *Acm Computing Surveys* (50:3), pp. 1-41.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age," *Journal of Consumer Psychology* (30:4), pp. 736-758.

Adjerid, I., Acquisti, A., and Loewenstein, G. 2019. "Choice Architecture, Framing, and Cascaded Privacy Choices," *Management Science* (65:5), pp. 2267-2290.
Adjerid, I., Peer, E., and Acquisti, A. 2018. "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," *MIS Quarterly* (42:2), pp. 465-488.
Aguirre, E., Mahr, D., Grewal, D.*, et al.* 2015. "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal Of Retailing* (91:1), pp. 34-49.
Al-Natour, S., Cavusoglu, H., Benbasat, I.*, et al.* 2020. "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research* (31:4), pp. 1037-1063.
Ayala, G. X., and Elder, J. P. 2011. "Qualitative methods to ensure acceptability of behavioral and social interventions to the target population," *Journal of public health dentistry* (71), pp. S69-S79.
Balaji, M., Khong, K. W., and Chong, A. Y. L. 2016. "Determinants of negative word-of-mouth communication using social networking sites," *Information & Management* (53:4), pp. 528-540.
Bartsch, M., and Dienlin, T. 2016. "Control your Facebook: An analysis of online privacy literacy," *Computers in Human Behavior* (56), pp. 147-154.
Baumeister, R. F., Bratslavsky, E., Finkenauer, C.*, et al.* 2001. "Bad is stronger than good," *Review of general psychology* (5:4), pp. 323-370.
Betzing, J. H., Tietz, M., vom Brocke, J.*, et al.* 2020. "The impact of transparency on mobile privacy decision making," *Electronic Markets* (30:3), pp. 607-625.
Brough, A. R., and Martin, K. D. 2019. "Critical roles of knowledge and motivation in privacy research," *Current opinion in psychology* (31), pp. 11-15.
Buckman, J. R., Bockstedt, J. C., and Hashim, M. J. 2019. "Relative Privacy Valuations Under Varying Disclosure Characteristics," *Information Systems Research* (30:2), pp. 375-388.
Buttle, F. A. 1998. "Word of mouth: understanding and managing referral marketing," *Journal of strategic marketing* (6:3), pp. 241-254.
Chang, H. H., Tsai, Y.-C., Wong, K. H.*, et al.* 2015. "The effects of response strategies and severity of failure on consumer attribution with regard to negative word-of-mouth," *Decision Support Systems* (71), pp. 48-61.
Chen, H., Li, X., Chiu, T.-S.*, et al.* 2021. "The impact of perceived justice on behavioral intentions of Cantonese Yum Cha consumers: The mediation role of psychological contract violation," *Journal of Hospitality and Tourism Management* (49), pp. 178-188.
Chih, W.-H., Chiu, T.-S., Lan, L.-C.*, et al.* 2017. "Psychological contract violation: Impact on perceived justice and behavioral intention among consumers," *International journal of conflict management* (28:1), pp. 103-121.
Fast, V. 2019. "The role of transparency in privacy decision-making under uncertainty," in *Proceedings of the 27th European Conference on Information Systems*, Stockholm & Uppsala, Sweden.
Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in online shopping: An integrated model," *MIS quarterly*), pp. 51-90.
Gerlach, J. P., Eling, N., Wessels, N.*, et al.* 2019. "Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy," *Information Systems Journal* (29:2), pp. 548-575.
Godinho de Matos, M., and Adjerid, I. 2021. "Consumer consent and firm targeting after GDPR: The case of a large telecom provider," *Management Science* (68:5), pp. 3330-3378.
Hair Jr., J. F., Hult, G. T. M., Ringle, C.*, et al.* 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*, Los Angeles: Sage.
John, L. K., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a plane: Context-dependent willingness to divulge sensitive information," *Journal of consumer research* (37:5), pp. 858-873.
Karwatzki, S., Dytynko, O., Trenz, M.*, et al.* 2017. "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* (34:2), pp. 369-400.
Keith, M. J., Babb, J., Furner, C.*, et al.* 2016. "Limited information and quick decisions: consumer privacy calculus for mobile applications," *AIS Transactions on Human-Computer Interaction* (8:3), pp. 88-130.
Kim, T., Barasz, K., and John, L. K. 2019. "Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness," *Journal Of Consumer Research* (45:5), pp. 906-932.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y.*, et al.* 2020. "The Effect of Fair Information Practices and Data Collection Methods on Privacy-Related Behaviors: A Study of Mobile Apps," *Information & Management*), pp. 103284.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y.*, et al.* 2021. "The Effect of Fair Information Practices and Data Collection Methods on Privacy-Related Behaviors: A Study of Mobile Apps," *Information & Management* (58:1), pp. 103284.

Liu, B., Pavlou, P. A., and Cheng, X. 2022. "Achieving a Balance Between Privacy Protection and Data Collection: A Field Experimental Examination of a Theory-Driven Information Technology Solution," *Information Systems Research* (33:1), pp. 203-223.

Malhotra, N. K., Sung, S. K., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Martin, K. D., Borah, A., and Palmatier, R. W. 2017. "Data privacy: Effects on customer and firm performance," *Journal of Marketing* (81:1), pp. 36-58.

Mehmood, S., Rashid, Y., and Zaheer, S. 2018. "Negative word of mouth and online shopping: Examining the role of psychological contract violation, trust and satisfaction," *Pakistan Journal of Commerce and Social Sciences (PJCSS)* (12:3), pp. 886-908.

Mohammed, Z. 2022. "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches," *Organizational Cybersecurity Journal: Practice, Process and People* (2:1), pp. 41-59.

Morey, T., Forbath, T., and Schoop, A. 2015. "Customer data: Designing for transparency and trust," *Harvard Business Review* (93:5), pp. 96-105.

Morrison, E. W., and Robinson, S. L. 1997. "When employees feel betrayed: A model of how psychological contract violation develops," *Academy of management Review* (22:1), pp. 226-256.

Nguyen, O. D. Y., Lee, J. J., Ngo, L. V.*, et al.* 2021. "Impacts of crisis emotions on negative word-of-mouth and behavioural intention: evidence from a milk crisis," *Journal of Product & Brand Management*.

Niehoff, B. P., and Paul, R. J. 2001. "The Just Workplace: Developing and Maintaining Effective Psychological Contracts," *Review of Business* (22.

Pavlou, P. A., and Gefen, D. 2005. "Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role," *Information systems research* (16:4), pp. 372-399.

Piccoli, G., and Ives, B. 2003. "Trust and the unintended effects of behavior control in virtual teams," *MIS quarterly*), pp. 365-395.

Reichheld, F. F., and Schefter, P. 2000. "E-loyalty: your secret weapon on the web," *Harvard business review* (78:4), pp. 105-113.

Robinson, S. L. 1996. "Trust and breach of the psychological contract," *Administrative science quarterly*), pp. 574-599.

Robinson, S. L., and Rousseau, D. M. 1994. "Violating the psychological contract: Not the exception but the norm," *Journal of organizational behavior* (15:3), pp. 245-259.

Rousseau, D. M. 1989. "Psychological and implied contracts in organizations," *Employee responsibilities and rights journal* (2:2), pp. 121-139.

Samat, S., Acquisti, A., and Babcock, L. 2017. "Raise the Curtains: The Effect of Awareness About Targeting on Consumer Attitudes and Purchase Intentions," in *Proceedings of the 13th Symposium on Usable Privacy and Security*, USENIX Association, pp. 299-319.

Schaub, F., Balebako, R., Durity, A. L.*, et al.* 2015. "A Design Space for Effective Privacy Notices," in *Proceedings of the Symposium on Usable Privacy and Security*, USENIX Association.

Selnes, F. 1998. "Antecedents and consequences of trust and satisfaction in buyer - seller relationships," *European Journal of marketing* (32:3-4), pp. 305-322.

Solove, D. J. 2013. "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* (126), pp. 1880.

Son, J.-Y., and Kim, S. S. 2008. "INTERNET USERS' INFORMATION PRIVACY-PROTECTIVE RESPONSES: A TAXONOMY AND A NOMOLOGICAL MODEL," *MIS Quarterly* (32:3), pp. 503-529.

Strycharz, J., Smit, E., Helberger, N.*, et al.* 2021. "No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies," *Computers In Human Behavior* (120), pp. 106750.

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. 2018. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law & Security Review* (34:1), pp. 134-153.

Trepte, S., Teutsch, D., Masur, P. K., *et al.* 2015. "Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS)," in *Reforming European data protection law*, Dordrecht: Springer, pp. 333-365.

Tsai, J. Y., Egelman, S., Cranor, L., *et al.* 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268.

Wang, W., and Wang, M. 2019. "Effects of sponsorship disclosure on perceived integrity of biased recommendation agents: Psychological contract violation and knowledge-based trust perspectives," *Information Systems Research* (30:2), pp. 507-522.

Wang, W., Xu, J., and Wang, M. 2018. "Effects of recommendation neutrality and sponsorship disclosure on trust vs. distrust in online recommendation agents: Moderating role of explanations for organic recommendations," *Management Science* (64:11), pp. 5198-5219.

Wetzer, I. M., Zeelenberg, M., and Pieters, R. 2007. ""Never eat in that restaurant, I did!": Exploring why people engage in negative word - of - mouth communication," *Psychology & Marketing* (24:8), pp. 661-680.

Williams, M., and Buttle, F. 2014. "Managing negative word-of-mouth: an exploratory study," *Journal of marketing management* (30:13-14), pp. 1423-1447.

Xu, H., and Zhang, N. 2021. "An Onto-Epistemological Critique of Information Privacy Research," in *Proceedings of Dewald Roode Workshop on Information Systems Security Research*, Texas.

Zarsky, T. Z. 2016. "Incompatible: The GDPR in the age of big data," *Seton Hall L. Rev.* (47), pp. 995.