Active Privacy Transparency: A Feasible Solution to Relieve the Escalating Tension Between Data Access and Privacy Protection

Early-stage 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-stage 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. More interestingly, it also ensures companies' immediate access to user data. Potentially, we expect this study to make important contributions to the growing body of research regarding privacy transparency and also, suggest a feasible way for companies to balance the increasing tension between privacy protection and data access.

[1] Corresponding Author

Keywords

Active privacy transparency, data access, privacy protection, psychological contract violation.

INTRODUCTION

The free processing of users' data is considered to be an essential driver for firms' development and innovation in the age of the digital economy (Godinho de Matos and Adjerid 2021). However, tensions arise between firms and consumers once a company's privacy practices are exposed by media (e.g., how data are collected and used by firms), even if the firm complies with privacy regulations. Accordingly, privacy-related news have 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). 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 and Robinson 1997; Pavlou and Gefen 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. This brings us to argue that privacy transparency might be a potential way to prevent the negative impacts of privacy-related news.

In current privacy practices, privacy transparency information is generally hidden in 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). In this manuscript, we focus on and design an *active* privacy transparency measure. 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 and eliminating information asymmetry between services providers and users (Godinho de Matos and Adjerid 2021). This is also more in line with the vision promoted by the latest privacy policies, such as the General Data Protection Regulation (GDPR) in the European Union[2] and the Personal Information Protection Law (PIPL) in China[3] are all placing sweeping new requirements on privacy transparency.

A primary obstacle for businesses to implement active privacy transparency is how it will influence companies' multiple and even competing privacy goals, such as privacy protection and information access. 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 literature on privacy transparency is ambiguous, different types of privacy transparency are not

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

[3] Please see http://www.gov.cn/xinwen/2021-08/20/ content _5632486.htm.

distinguished, and findings on privacy transparency impact are highly inconsistent. Specifically, one stream of work finds that explicitly informing users about data practices can help companies earn ongoing even expanded data access, increase user service adoption, and even release the drop in firm stock price (Aguirre et al. 2015; Godinho de Matos and Adjerid 2021; Martin et al. 2017; Wang et al. 2018). In contrast, substantial studies argue that active privacy transparency makes privacy risk more explicit, reduces user information disclosure, and even stalls innovation of the whole society in the era of big data (John et al. 2011; Keith et al. 2016; Kim et al. 2019; Zarsky 2016). Additionally, some studies show that increased transparency features do not significantly alter individuals' privacy attitudes and behaviors, and the underlying reasons remain unclear (Betzing et al. 2020; Karwatzki et al. 2017; Strycharz et al. 2021).

Given the privacy dilemma companies face and conflicting findings surrounding transparency impact, we propose and design an active privacy transparency measure and investigate its immediate and profound impacts on companies. Specifically, we aim to answer 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?

RELATED LITERATURE

What is Privacy Transparency

Privacy transparency has become a trending topic of discussion and is attached to great importance by policymakers and consumer privacy advocates (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), and it has been further explained in previous literature 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 and Adjerid 2021).

In current practice, how to establish and display privacy transparency is largely at the discretion of online service providers (Betzing et al. 2020), and thus 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". The passive privacy transparency is neither usable nor useful in protecting user privacy and eliminating information asymmetry (Schaub et al. 2015). Therefore, this paper focuses on active privacy transparency relative to passive privacy transparency.

The Effects of Privacy Transparency

The existing literature is ambiguous on how active privacy transparency will influence individuals' immediate and long-term privacy behaviors. First, the current research findings on privacy transparency are inconsistent. Some studies found that the impacts of privacy transparency are positive and promotional. For example, Morey et al. (2015) proposed that privacy transparency is a tactic to help companies earn ongoing data access from users, and this view was supported by the field experiments conducted by Godinho de Matos and Adjerid (2021). Martin et al. (2017) even found that the firm that provided higher privacy transparency suffered a smaller drop in stock price after a data breach. Such studies shared a common explanation that privacy transparency is a signal of trust, and higher transparency could build trust and decrease vulnerability. However, many studies found contrary effects. For example, some scholars argue that when people are offered privacy transparency, they tend to deny privacy permission and reduce information disclosure (John et al. 2011; Keith et al. 2016).

Moreover, previous work highlighted that revealing privacy transparency decreases the effectiveness of targeted advertisements, and it is particularly true when the information flows are unacceptable, or consumers' original opinion toward the targeted ad is negative (Kim et al. 2019; Samat et al. 2017). Zarsky (2016) predicted that the enhanced privacy transparency requirement is incompatible with the development of big data and artificial intelligence and will even hinder the innovation of the whole society. The common mechanism underlies this stream of work is that privacy transparency is a risk signal that makes privacy concerns more explicit and prominent. More interestingly, some recent research has found that the privacy transparency feature does not significantly shape users' privacy decision-making, such as information disclosure, permission granting and privacy protection motivation (Betzing et al. 2020; Karwatzki et al. 2017; Strycharz et al. 2021).

Second, existing literature only focuses on the impact of privacy transparency on a certain behavior or in a specific aspect, such as information disclosure or privacy protection. Organizations have multiple privacy needs that are often even competing. As the saying goes, "a slight move in one part may affect the whole situation" privacy transparency may have complex impacts and play different roles in fulfilling companies' competing demands. However, this systemic 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 and Zhang (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. Through the semi-structured interviews with board-level executives and product managers, 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.

HYPOTHESES DEVELOPMENT

Profound Effect of Privacy Transparency

Forbes Insight Report[4] shows that issues related to information privacy and security have the potential to do the most damage to companies' reputations. 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 and Schefter 2000; Selnes 1998). Once they are damaged, the negative impacts could last for a long time. Therefore, we focus on the NWOM and trust decline and use them as proxies to characterize the profound effects.

In a broader context of buyer-seller relationship building, academics and practitioners alike have suggested that the most important predictor of negative outcomes, especially the generation of NWOM and decline in trust, is users' perceived psychological contract violation (Chen et al. 2021; Pavlou and Gefen 2005; Wang et al. 2018). As such, we examine whether active privacy transparency could mitigate these negative outcomes triggered by privacy-related news from a theoretical perspective of the psychological contract violation (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, and there are two primary causes of PCV: incongruence and reneging (Pavlou and Gefen 2005).

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

Incongruence means that two parties have different understandings of the psychological contract (Morrison and Robinson 1997). In the context of our research, the incongruence largely stems from the fact that users and service providers have different knowledge and information on how personal data is processed in businesses' privacy practices (Acquisti et al. 2017; Acquisti et al. 2020). After implementing the active privacy transparency, businesses' privacy practices will be clearly notified to users. This can clarify and update users' privacy understanding and knowledge and thus reduce privacy uncertainty and information asymmetry (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, NWOM is an outcome of an imbalance between individuals' expectations and perceptions (Buttle 1998), 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 unable or unwilling to do so (Morrison and Robinson 1997). In the context of our study, the reneging manifests as service providers intentionally hiding their privacy practices due to opportunism. Active privacy transparency allows companies to proactively disclose their information practices by themselves before users make privacy decision (Betzing et al. 2020; Godinho de Matos and Adjerid 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. Unlike incongruence, a typical feature of reneging is knowingly failing to fulfill the contract (Morrison and Robinson 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 and Paul (2001) revealed that reducing PCV is critical to rebuilding trust with employees. Piccoli and Ives (2003) found that trust decline in virtual teams is rooted in PCV caused by reneging. Wang and Wang (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 could inherently lead to a drop in trust. We argue that after providing active privacy transparency, it will also show a decrease in users' trust, but the decline will be mitigated, 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 Effect of Privacy Transparency

Regarding immediate effects, the most direct and crucial to businesses is how active privacy transparency will influence user information disclosure (Gerlach et al. 2019). However, as mentioned above, this issue is still ambiguous in extant literature and open to debate (Godinho de Matos and Adjerid 2021). In essence, these inconsistent findings can be primarily summarized as a controversy over the dual feature of privacy transparency: privacy risk versus trust. Some studies find that privacy transparency increases users' perceived privacy risk and thus has a chilling effect on their information disclosure (John et al. 2011; Keith et al. 2016); some studies argue that transparency information is beneficial for trust-building and leads to an increase in user data allowances (Aguirre et al. 2015; Morey et al. 2015); and others suggest that the dual mechanisms may work together, resulting in an insignificant effect of privacy transparency on information disclosure (Karwatzki et al. 2017).

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:

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

We designed an active privacy transparency measure and conducted a controlled two-stage laboratory experiment to test the proposed hypotheses.

Pre-test

The pre-test aims to select content of privacy transparency used in the formal experiment.

Transparency Content Generation. We used the privacy setting of m-commerce's personalized recommendation as our experimental scenario. First, we summarized information privacy practices about the personalized recommendation function from the privacy policies of the Top 5 m-commerce Apps in China. Then, according to the definitions of privacy transparency in prior literature (Godinho de Matos and Adjerid 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 are often associated with privacy practices that are inconsistent with users' original perception and therefore have low user acceptance (Kim et al. 2019). These privacy practices are also companies worry about most in implementing active privacy transparency. Thus, we recruited 77 participants and asked them to rate the acceptability of each item in the selection set of privacy transparency. The item with the lowest score is 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). The post-hoc full pairwise comparisons indicated that participants have the lowest acceptability of transparency information about data collection than any other four items. Therefore, the item of data collection will be used as privacy transparency text in the following experiment.

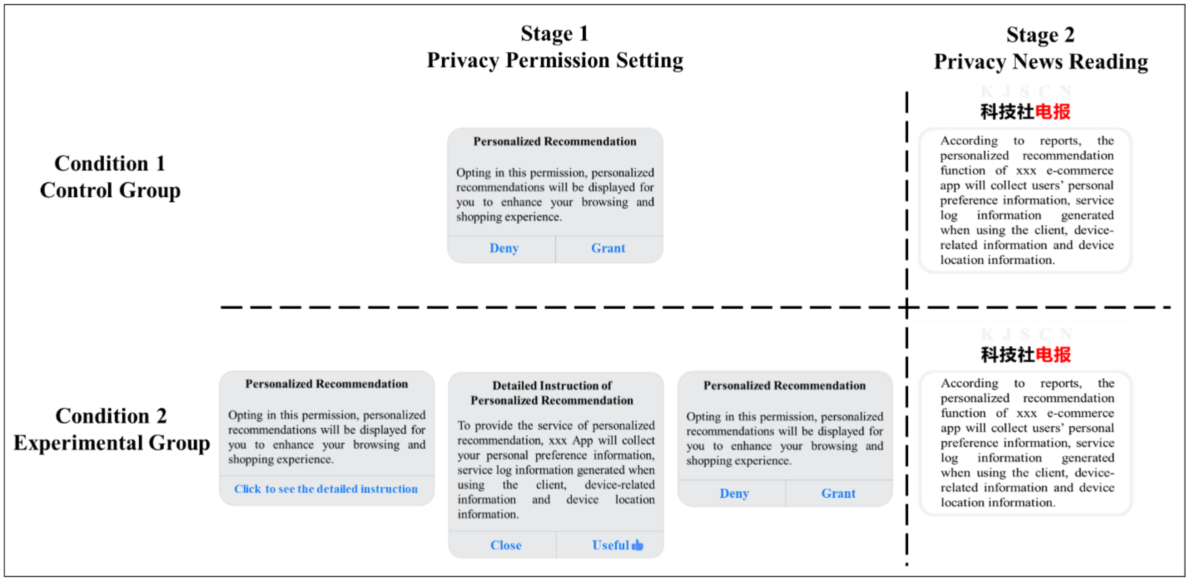
Experimental Design

Our investigation of some popular m-commerce applications 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, as shown in Figure 1 (condition 2). Specifically, we first changed the personalized recommendation from a default function to opt-in permission presented in 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. This design addresses the problems that the current passive privacy transparency has in the following ways: (1) In the first interface, there is only one option of "click to read the transparency information", which solves the problem of unknowing caused by users not reading the privacy policy; (2) The transparency content is directly linked to permission decisions, giving users actual control on their privacy; (3) This design indeed informs users privacy transparency information in a proactive way, rather than being used as a method to abide by privacy regulations passively. In this study, we employed a one-factor between-subjects design, where condition 1 was not given transparency information, and condition 2 adopted our new design of active privacy transparency (see Figure 1).

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 the procedure of our study. Next, participants were randomly assigned to the two experimental conditions and finished a two-stage task. In stage 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 any other app. Soon after opening the app, a permission setting notification for 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 condition 1 just needed to decide whether to grant or deny the personalized recommendation permission request as usual, while people in condition 2 were required to read the privacy transparency information and evaluate whether the content was useful before deciding to enable or close this privacy permission. Then, the first-task task was completed, and participants in two groups were asked to fill a post-task questionnaire. In stage 2, we reported the transparency information behind the beta app's personalized recommendation in the form of news (same content as in stage 1), stimulating companies' privacy practices exposed by the media. All participants were required to read the same news and complete the stage 2 post-task questionnaire.



Personalized Recommendation

Opting in this permission, personalized recommendations will be displayed for you to enhance your browsing and shopping experience.

Detailed Instruction of Personalized Recommendation

To provide the service of personalized recommendation, xxx App will collect your personal preference information, service log information generated when using the client, device-related information and device location information.

According to reports, the personalized recommendation function of xxx e-commerce app will collect users' personal preference information, service log information generated when using the client, device-related information and device location information.

Figure 1. Experimental Flow.

Measurement

Our experimental measurements consist of two parts. One part is users' actual behavioral data recorded by our self-developed app. During the task, 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. In the stage 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, perceived privacy risk of the privacy permission (Libaque-Sáenz et al. 2021), and trust in the app (Liu et al. 2022). Last, we included questions to check the manipulation of privacy transparency (Martin et al. 2017; Wang et al. 2018). In the stage 2 questionnaire, we measured participants' negative word of mouth (Martin et al. 2017) and perceptions of psychological contract violations (Pavlou and Gefen 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 collected (Malhotra et al. 2004).

DATA ANALYSES AND RESULTS

Profound Effects

We first analyzed participants' responses in the second-stage task to examine the impact of privacy transparency on profound WOM and Trust. 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 stage1 minus that in stage 2, and used it to characterize the changes in users' trust. Table 1 presents the results. The results 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 privacy transparency information proactively could effectively reduce NWOM 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 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 1. Main Effects of Privacy Transparency on NWOM and Trust Decline

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

Immediate Effects

Next, we analyzed participants' responses in the first-stage task to investigate the impact of privacy transparency on immediate information disclosure? We conducted a binary logistic regression to test the immediate effect of privacy transparency. Users' actual choice of the privacy permission in the first-stage task was used as the dependent variable to reflect user privacy disclosure. Unlike the negative impact we hypothesized, the results 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 disclosure behavior notably. Hence, H3 was not supported by the data.

DISCUSSION AND EXPECTED CONTRIBUTIONS

Research Summary and Key Findings

Addressing the escalating tension between privacy protection and data access is a critical and urgent issue facing companies in the current era. Our study sought to provide insight into this question by designing an active privacy transparency measure and exploring its role in fulfilling companies' competing privacy needs. We yielded several important findings. First, results of the second stage 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 NWOM 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 stage 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 disclosure decision does not decrease significantly. At face value, our study suggests that users' information disclosure 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, in the future analysis, we plan to perform in-depth analyses on the insignificant immediate impact to provide an insightful explanation for the current inconsistent findings of privacy transparency.

Expected Theoretical Contributions

Our study is expected to make important contributions to the growing body of research regarding privacy transparency. First, we will 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, which will help avoid research confusion caused by scopes and provide 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 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 and Zhang 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 will fill this gap by exploring the impact of privacy transparency on the two competing privacy needs companies are concerned about most: long-term privacy reputation and users' trust versus immediate data access. Lastly, our planned further analysis underlying the insignificant immediate effect will explore plausible moderators, which has the potential to provide insightful explanations for the current inconsistent findings of privacy transparency.

Expected 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 privacy protection and data access. 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. From a policy perspective, our results call for fine-grained requirements for privacy transparency, 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 several 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. Therefore, in the following study, we plan to expand the sample size to improve the stability of our findings. Second, 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). Finally, this study aims to consider the privacy needs of both users and firms, and ultimately seek a win-win solution to the current privacy dilemma. In our research, the win-win idea is reflected as: for users, we proposed and designed an active privacy transparency measure from a user privacy-friendly perspective; for service providers, we investigated the impact of the such measure on their immediate data access and long-term privacy-related reputation. However, the impacts on the business are still reflected by the data collected from the user side only. In the future study, we intend to conduct field experiments to capture actual outcomes from the organizational side, and thus provide more comprehensive evidence on the effectiveness of active privacy transparency in mitigating the privacy tension between users and service providers.

ACKNOWLEDGEMENTS

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

REFERENCES

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., *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., de Ruyter, K., *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., and Aleem, U. 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.

Baumeister, R.F., Bratslavsky, E., Finkenauer, C., and Vohs, K.D. 2001. "Bad Is Stronger Than Good," *Review of general psychology* (5:4), pp. 323-370.

Betzing, J.H., Tietz, M., vom Brocke, J., and Becker, J. 2020. "The Impact of Transparency on Mobile Privacy Decision Making," *Electronic Markets* (30:3), pp. 607-625.

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.

Chen, H., Li, X., Chiu, T.-S., and Chen, F. 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., and Fang, W.-C. 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," *Proceedings of the 27th European Conference on Information Systems*, Stockholm & Uppsala, Sweden.

Gerlach, J.P., Eling, N., Wessels, N., and Buxmann, P. 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.

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., and Veit, D. 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., Abdullat, A., *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., and Bravo, E.R. 2021. "The Effect of Fair Information Practices and Data Collection Methods on Privacy-Related Behaviors: A Study of Mobile Apps," *Information & Management* (58:1), p. 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.

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.

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," *Proceedings of the 13th Symposium on Usable Privacy and Security*, USENIX Association, pp. 299-319.

Schaub, F., Balebako, R., Durity, A.L., and Cranor, L.F. 2015. "A Design Space for Effective Privacy Notices," *Proceedings of the Symposium on Usable Privacy and Security*, USENIX Association: 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), p. 1880.

Strycharz, J., Smit, E., Helberger, N., and van Noort, G. 2021. "No to Cookies: Empowering Impact of Technical and Legal Knowledge on Rejecting Tracking Cookies," *Computers In Human Behavior* (120), p. 106750.

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.

Xu, H., and Zhang, N. 2021. "An onto-Epistemological Critique of Information Privacy Research," *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), p. 995.