

The Effect of Environmental Perception on Young People's Willingness to Continue Use of Digital Services in the Digital Transformation Era

Xinyue Li

*Economics, Boston University, Boston, USA
lio@bu.edu*

Abstract. This study focuses on the effect of Chinese young people's perception of the private information regulation environment on their willingness to continue using the digital services provided by businesses. The model is inspired by the APCO model, and the study also uses the ABC model to explain the inconsistency. According to a questionnaire survey with 100 valid responses from Chinese young people aged 18 to 28, ordinary least squares regression analysis and bootstrap mediation analysis were conducted. The analysis shows that environmental perception has a significant positive effect on individuals' willingness to disclose private information. With a perceived privacy environment as secure and well-regulated, the respondents are encouraged to provide their private information. However, the result shows that the environmental perception does not significantly affect continued usage intention. Moreover, the willingness to disclose their information is unable to mediate the relationship between environmental perception and the young people's willingness to continue using the digital services. These findings indicate that although the relationship between consumers' perceptions of the privacy environment and their disclosure behavior is positive, it may not be sufficient to increase continued usage of digital services. Continued usage intention may also depend on other factors, such as perceived usefulness, convenience, and habit. This paper contributes to the privacy issues by introducing environmental perception as an important antecedent variable, and examining its influence on consumers' privacy-related behavior in digital environments.

Keywords: Digital Transformation, Personal Information, Environmental Perception, APCO

1. Introduction

Digital transformation has gradually become an important trend in most industries over the past decade. Recent research shows that there are more than 90% of organizations experiencing digital transformation [1]. However, it also brings increasing concerns about personal data privacy protection. Consumers' personal information may be exposed to different risks, such as online tracking, targeted advertising, and unauthorized data sharing [2]. At the same time, firms are collecting and processing more personal data than before, sometimes with consumers' clear consent

while other times not. Thus, privacy has become an important issue in planning both marketing and digital business strategies [3].

In order to prevent enterprises from misusing personal information, there are many countries and governments enact privacy regulations to improve consumer protection and maintaining consumer rights and interests. For example, the General Data Protection Regulation (GDPR) implemented in 2018, and it requires firms to obtain explicit consent before collecting and processing user data, and also sets strict rules on data usage [4]. Another example is the California Consumer Privacy Act (CCPA). It provides consumers with more rights to access, control, and limit how businesses use their personal information [5]. These regulations show that governments are making efforts to protect privacy under the current digital economy environment. Although these legal protections show that governments really care about consumers' right, privacy risks still exist due to the complexity and scale of digital business models. As a result, consumers are now paying more attention to privacy issues and are becoming more sensitive to how firms collect and use their personal information.

This shift brings a new challenge to firms, that is, how to balance between the personalized services, consumers acknowledgement to their data rights and privacy control. When consumers perceive that their personal information may be at risk, they will trust firms and platforms less and reduce their use of them. Previous studies support this argument and suggest that stronger privacy protection can increase consumer trust and, in turn, encourage people to provide personal information [6, 7]. Meanwhile, the adaptation of these privacy regulations require firms to pay for additional costs to avoid from being fined while retaining their consumers and updating their data collection and personalized marketing strategies. Although these studies give useful insights, most of them only focus on the supply side, especially for the firms' ability to collect data and the extra compliance costs. Comparatively less attention is paid to the demand side, particularly to the way that consumers perceive the privacy environment and how these perceptions shape their behavioral decisions. Thus, privacy regulation may not influence behavior directly. Instead, it may operate through consumers' perceptions of data protection and the resulting willingness to share private information.

The problem shown above promotes this practical research. This paper uses the Antecedent-Privacy Concerns-Outcomes (APCO) framework, and it proposes the consumer-side reasons for considering privacy concerns, such as self-efficacy, awareness of big data, and perceived control [8]. This mechanism shows that these antecedent individual perceptions can lead to privacy concerns and further influence trust and self-disclosure behavior. While the APCO model refers to the importance of personal awareness, it does not explicitly consider the function from regulatory agencies and firms' data usage in reality to the external privacy environment. In the real world, consumers do not simply respond to general privacy concerns, but also evaluate whether the surrounding environment provides sufficient protection for their personal data.

This paper is inspired by the APCO framework and introduces environmental perception as a key independent variable. Environmental perception is identified as personal understanding of the privacy surroundings and their confidence, including government regulation and firms' data practices. To be more specific, it is whether consumers trust the business and regulations and in turn willing to provide their data to them. The research proposes that environmental perception may influence consumers' willingness to provide personal information, and this may affect their intention to continue using. Therefore, the mediating variable is willingness to provide personal information, and it connects the environmental perception and continued use in this framework. This mechanism

is shown in Figure 1. One of the previous studies also suggests that perceived privacy protection and trust can influence disclosure behavior, supporting this proposed mechanism [9].

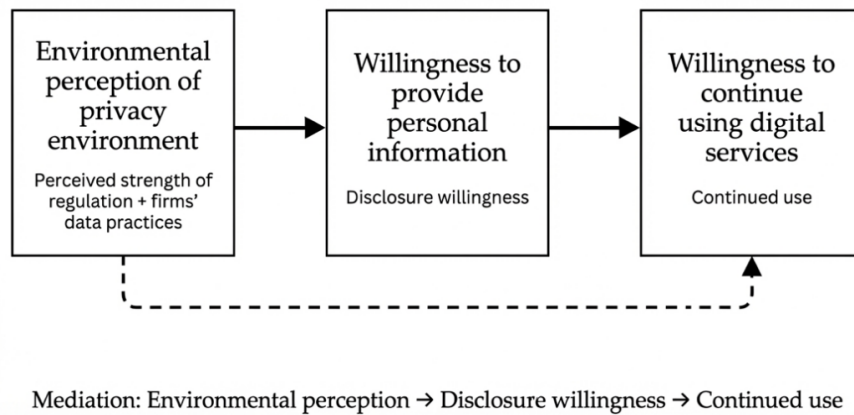


Figure 1. Mechanism

Based on this framework, this paper focuses on the research question: how does an individual's perception of the privacy environment influence their willingness to provide personal information and their willingness to continue using digital services? More specifically, the study examines whether stronger perceived privacy protection can allow consumers to share personal information and whether it is related to continued use of digital services. The research paper is trying to offer a new aspect of how privacy regulation affects consumer behavior from the demand side. To examine these relationships, a questionnaire survey was conducted to measure several key constructs about environmental perception, willingness to disclose personal information, and willingness to continue use. After that, the study applies ordinary least squares regression(OLS) and bootstrap mediation analysis to test the relationships among these variables and the proposed mediation mechanism. The findings are trying to contribute to the APCO framework and also provide practical implications for firms that are trying to develop more privacy-sensitive digital strategies.

2. Literature review

As consumer data are used broadly in digital environments, privacy has gradually become an important issue in understanding consumer behavior. Although regulations like GDPR and CCPA are designed to improve consumer protection and businesses' initiatives, past studies suggest that consumers' responses to privacy are not influenced only by formal regulations, but also by how they perceive the overall privacy environment [3]. Smith et al. point out that consumers become more sensitive when firms collect and process personal information without sufficient transparency or protection [10]. As people know more about the risks of the misuse of their private data, it becomes really crucial to understand how these perceptions shape their decisions. Consumers may worry about unwanted marketing communications, online tracking, and potential invasions of privacy [3]. These concerns may reduce trust in digital platforms and influence their behavioral intentions.

2.1. Defining Information Privacy Concerns (IPC)

The cornerstone of privacy research is the concept of information privacy concerns. Malhotra, Kim, and Agarwal propose the Internet Users' Information Privacy Concerns (IUIPC) framework. It views concerns of the privacy as a multidimensional construct, ranging from data collecting, controlling, to consciousness of privacy practices [11]. Their findings manifest that consumers' concerns have a significant influence on behavioral intentions to authorize personal information. It means that higher levels of privacy concerns can reduce individuals' willingness to share information online. In their statistical analysis, the authors find that higher levels of IUIPC negatively affect trusting beliefs ($\beta = -0.34, p < .001$), and then reduce consumers' willingness to disclose their personal information on the Internet [11]. This proves that the individual perceptions plays an important role in deciding whether disclose personal information or not. Aside from this, trust, an abstract psychological concept that is totally subjective, has also been viewed as a central mechanism in connecting the environmental perception and consumers' behaviors. McKnight et al. deem that trust can reduce uncertainty and perceived risk online. It makes consumers more willing to engage in trust-related behaviors, such as sharing personal information or executing online transactions [12]. Institution-based trust, such as regulations, technological safeguards, and legal protections, is equally indispensable in shaping individuals' willingness to participate in digital activities. When consumers perceive the privacy environment as secure and well-regulated, they are generally more likely to trust platforms and disclose personal information.

2.2. Inconsistency

Existing studies provide different explanations for how the privacy-related perceptions affect consumer behavior in the digital environment. On the one hand, some studies suggest that when people feel the privacy environment as safe and secure, they tend to trust the digital platforms and disclose their personal information in such services [13]. McKnight, Choudhury, and Kacmar argue that institution-based trust reduces uncertainty and perceived risk online [12]. Similarly, Degutis et al. find that the reliance on e-commerce platforms significantly promotes individuals' willingness to disclose personal data [6]. On the other hand, another group of researchers emphasizes that the increasing awareness of data collection and privacy safety may strengthen privacy concerns and reduce disclosure willingness. Malhotra, Kim, and Agarwal demonstrate that stronger Internet privacy concerns negatively affect consumers' intentions to provide their privacy information [11]. Martin and Murphy further argue that consumers become more cautious when firms collect personal information without sufficient transparency or protection [3].

To better explain these inconsistent findings, this study uses the Antecedent–Behavior–Consequence (ABC) framework [14]. In this framework, consumers' perception of the privacy environment serves as the antecedent, the behavioral response is willingness to provide personal information, and willingness to continue using digital services functions as the behavioral outcome. Based on this framework, the study proposes that environmental perception may influence continued usage intention indirectly through disclosure willingness. All of these explanations lead to the following hypothesis.

Hypothesis 1. There is a positive relationship between perception of the privacy environment and consumers' willingness to disclose their personal information.

Hypothesis 2. Consumers' willingness to disclose personal information is positively associated with their intention to continue using digital services.

Hypothesis 3. The willingness to disclose personal information mediates the positive relationship between perceived privacy environment and consumers' continued usage intention.

3. Methodology

The study uses an online questionnaire survey to examine the relationship between consumers' perception of the privacy environment, willingness to provide personal information, and willingness to continue using digital services. The responses are mostly from Chinese young people, aged from 18 to 28. Among those respondents, half of them are international students studying in the U.S., while the rest of them are studying or living in China. Based on the ABC framework, the antecedent is environmental perception, disclosure willingness represents the behavioral response, and the behavioral outcome is continued usage intention.

The survey was distributed and collected through social media platforms and personal networks, yielding 100 valid responses. For the basic demographic information, it contains age, education level, and frequency of Internet use as control variables. Environmental perception was measured using items related to privacy regulation and firms' data protection practices, which were adapted from Degutis et al., Malhotra, Kim, and Agarwal, and so on, and the Cronbach's Alpha test scores are shown in Table 1 [6, 11, 12, 15, 16]. The Cronbach's Alpha test was conducted to assess the internal consistency of the measurement scales. In Table 1, all the scores are above 0.7, indicating satisfactory reliability. The measurement of willingness to provide personal information was based on respondents' intention to disclose different types of personal information, such as names, emails, browsing history, and address, in exchange for discounts or personalized services. Continued usage intention was measured through respondents' willingness to continue using websites or applications under different situations. Each of the questionnaire questions is scaled from 1(strongly disagree) to 5(strongly agree). After data collection, ordinary least squares (OLS) regression and mediation analysis were conducted to examine the connections among those variables and test the proposed mediation mechanism.

Table 1. Questionnaire questions and Cronbach's Alpha test

Construct	Questionnaire Items	Source	Cronbach's Alpha Test
Environmental Perception (IV)	EP1. I believe current regulations strongly constrain firms' collection and use of personal data.	Degutis et al. (2023)	0.840
	EP2. If a company misuses my data, I know which authority I can report it to.		
	EP3. Current privacy laws effectively protect my personal data and privacy.		
	EP4. I am familiar with privacy protection regulations in my country or region.		

Table 1. (continued)

Willingness to Provide Personal Information (Mediator)	EP5. Companies should clearly disclose how personal data are collected and used.		
	EP6. Companies should provide clear and understandable privacy policies.		
	EP7. I should know how my private information is being used.	Malhotra et al. (2004)	
	DW1. Willingness to disclose real name.		0.942
	DW2. Willingness to disclose age/date of birth.		
	DW3. Willingness to provide gender.		
	DW4. Willingness to give phone number.		
Continued Usage Intention (DV)	DW5. Willingness to give email address.		
	DW6. Willingness to share browsing history.		
	DW7. Willingness to disclose home address.	Degutis et al. (2023)	
	CU1. I intend to continue using the websites/apps I currently use.	McKnight et al. (2002); Fortes & Rita (2016)	0.824
	CU2. Even if a platform experiences a data breach that does not affect my property or personal safety, I would continue using it.	Fortes & Rita (2016)	
	CU3. I am reluctant to switch to new websites or apps.	Limayem et al. (Habit in IS Continuance)	

4. Results

The regression and mediation results are summarized in Table 2. Model (1) reports the relationship between environmental perception and willingness to provide personal information, while Model (2) includes the willingness to provide personal information as the mediator. The final section presents

the mediation analysis for continued usage intention. Table 2 presents the OLS regression analysis, and Table 3 represents the bootstrap mediation analysis.

Table 2. Regression analysis

	Willingness to Provide Personal Information	Continued Usage Intention
Variables	Model 1 b (SE)	Model 2 b (SE)
Environmental Perception	0.362** (0.134)	0.060 (0.068)
Willingness to Provide Personal Information	—	0.010 (0.056)
R ²	0.115	0.021
Adjusted R ²	0.099	-0.020

Notes. Standard errors are reported in parentheses.

* $p < .05$, ** $p < .01$.

Effect of environmental perception on willingness to provide personal information

In Model (1), environmental perception has a positive and significant effect with significance on the willingness to provide personal information ($B = 0.362$, $p = .009$). Respondents who perceive the privacy environment as more secure have more intention to provide their personal information. Therefore, H1 is supported. However, Model 2 shows that when predicting the outcome variable, Continued Usage Intention, neither Environmental Perception ($B = 0.060$, $p = .389$) nor Willingness to Provide Personal Information ($B = 0.010$, $p = .855$) yields statistical significance. The explanatory power of Model 2 is extremely low, suggesting that these privacy-related factors fail to explain young consumers' continuance intentions. Thus, Hypothesis 2 is not supported.

Mediation Analysis for Willingness to Provide Personal Information

According to the bootstrap mediation analysis presented in Table 3, the indirect effect of environmental perception on willingness to provide personal information is significant (Indirect effect = 0.116, BootSE = 0.059, 95% CI [0.019, 0.251]). Since zero is not in the confidence interval, the mediation effect is statistically significant.

Table 3. Bootstrap mediation analysis

Outcome Variable	Indirect Effect	Boot SE	95% CI
Continue Usage Intention	0.005	0.024	[-0.043, 0.054]

Mediation Analysis for Continued Usage Intention

To test the proposed mediation mechanism (Hypothesis 3), a bootstrap mediation analysis with 3,000 resamples were conducted. In Table 3, the indirect effect of environmental perception on continued usage intention through willingness to provide personal information is 0.005 (Boot SE = 0.024). Since the 95% confidence interval [-0.043, 0.054] includes zero, the mediation effect is statistically insignificant. Therefore, Hypothesis 3 is not supported.

5. Discussion

Analyzing survey data collected from 100 respondents, this study examines how consumers' perception of the privacy environment influences their willingness to provide personal information and their intention to continue using digital products. A distributed questionnaire was administered to young Chinese people aged 18 to 28 across the region. Half of them were studying in the US, and the other half were living and studying in China. At the end of the analysis, the findings support hypothesis 1 but not H2 or H3.

The results of the analysis show that environmental perception has a significant positive effect on willingness to provide personal information ($B=0.362$, $p=.009$). This finding suggests that consumers who perceive the privacy environment as secure and well regulated are more willing to share personal information, supporting H1. This result is consistent with previous studies arguing that trust and perceived privacy protection reduce perceived risks and encourage information disclosure in digital environments [3, 12].

However, the proposed mediation mechanism (H3) and the direct relationship between disclosure willingness and continuance intention (H2) are not supported. According to Model 2, when predicting continued usage intention, neither environmental perception ($B = 0.060$, $p > .05$) nor the willingness to provide personal information ($B = 0.010$, $p > .05$) yields statistical significance. Furthermore, the bootstrap mediation analysis supports the indirect effect of environmental perception on continued usage intention through the personal information disclosure willingness is 0.005. The 95% confidence interval is $[-0.043, 0.054]$. Because the confidence interval includes zero, the mediation effect is statistically insignificant. It means that H2 and H3 are not supported. There is a possible explanation that continued usage behavior may also depend on other additional factors, such as platform usefulness, convenience, habit, or entertainment value [16, 17]. Further research is still required to add those possible influential variables. Therefore, while a positive perception of the privacy environment successfully encourages initial or transaction data disclosure, it is insufficient to drive long-term, continuous digital service adoption.

6. Conclusion

This study contributes to the current privacy field in several directions. First, it is inspired by the APCO framework by introducing environmental perception as an important antecedent variable. Also, it applies the ABC framework to interpret how privacy-related perceptions can influence digital behavior through disclosure willingness. Lastly, this study shifts attention from firm-level privacy regulation to consumers' subjective perception of the privacy environment. Although this study shows no effect between the environmental perception and the continued usage intention, there are still some realistic benefits. For firms, providing consumers with a safe environment is still important in increasing their trustworthiness and the stickiness of consumers. The official regulations are only the starting point, and the more realistic state is how firms adjust their strategies. On the other side, with the much more complex Internet use and digital transformation, improving people's awareness to protect personal information is also significant. However, this paper also has some limitations. The sample size is relatively small ($N = 100$), and the questionnaire was distributed mainly through online personal networks, where the generalizability of the result might be limited. Also, the study uses cross-sectional survey data, which means it is hard to establish strong causal relationships, but only the relationships between the variables are provided. Future research needs to use larger samples or longitudinal designs to further examine consumer behavior in digital environments.

In conclusion, this study emphasizes consumers' perceptions of the privacy environment in cultivating disclosure willingness. Meanwhile, the findings suggest that continued usage intention may be influenced by motivations beyond privacy-related concerns. Even though there is no significance in the continued usage intention of digital services, this might be due to other factors that are not taken into consideration in this research. Thus, future research may incorporate additional factors, such as perceived usefulness, habit, and platform value, so that continued digital service usage can be explained much more deeply and comprehensively.

References

- [1] McKinsey & Company. (2026, April 6). Author talks: Rewiring to outcompete with AI. *McKinsey & Company*. <https://www.mckinsey.com/featured-insights/mckinsey-on-books/rewired>
- [2] Hicklen, H. (2026). Consumers care deeply about data security and privacy, but are they doing enough to protect their information? <https://clutch.co/resources/consumer-data-security-privacy#corporate-responsibility-to-protect-consumer-data>
- [3] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/10.1007/s11747-016-0495-4>
- [4] GDPR.eu. (n.d.). What is GDPR, the EU's new data protection law? *GDPR.eu*. <https://gdpr.eu/what-is-gdpr/>
- [5] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018). https://cippa.ca.gov/regulations/pdf/ccpa_statute.pdf
- [6] Degutis, M., Urbonavičius, S., Hollebeek, L. D., & Anselmsson, J. (2023). Consumers' willingness to disclose their personal data in e-commerce: A reciprocity-based social exchange perspective. *Journal of Retailing and Consumer Services*, 74, 103385. <https://doi.org/10.1016/j.jretconser.2023.103385>
- [7] Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2023). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing*, 28(2), 337–357. <https://doi.org/10.1057/s41264-022-00154-z>
- [8] Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, 41(1), 62–96. <https://doi.org/10.17705/1CAIS.04104>
- [9] Fox, G. (2021). Understanding and enhancing consumer privacy perceptions in the cloud. In M. Gupta & R. Sharman (Eds.), *Data privacy and trust in cloud computing* (pp. 59–78). Springer. https://doi.org/10.1007/978-3-030-54660-1_4
- [10] Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–A27. <https://doi.org/10.2307/41409970>
- [11] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355.
- [12] McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- [13] Bansal, G., Zahedi, F. "Mariam", & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138–150. <https://doi.org/10.1016/j.dss.2010.01.010>
- [14] Catania, A. C. (2003). B. F. Skinner's science and human behavior: Its antecedents and its consequences. *Journal of the Experimental Analysis of Behavior*, 80(3), 313–320. <https://doi.org/10.1901/jeab.2003.80-313>
- [15] Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, 22(3), 167–176. <https://doi.org/10.1016/j.iedeen.2016.04.002>
- [16] Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, 31(4), 705–737. <https://doi.org/10.2307/25148817>
- [17] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>