Issues in Information Systems
Volume 26, Issue 2, pp. 323-334, 2025

DOI: https://doi.org/10.48009/2_iis_125

Cross-cultural privacy literacy in E-commerce: Testing users' understanding of platform data practices

Jing Hua, *La Roche University, jing.hua@laroche.edu*
Ping Wang, *Robert Morris University, wangp@rmu.edu*

Abstract

This study investigates users' declarative knowledge of data collection practices on e-commerce platforms in different cultures, focusing on Amazon in the United States and Taobao in China. Unlike prior research emphasizing general privacy awareness or technical skills, this study examines platform-specific knowledge of what data is collected—an essential but often overlooked aspect of privacy literacy. Data from 318 Amazon users and 189 Taobao users were analyzed using chi-square tests across multiple data types. A five-pint Likert scale was employed to assess users' knowledge objectively and reduce potential inaccuracies associated with self-reported bias. Results show that Taobao users demonstrated significantly greater accuracy in identifying platform data collection practices, particularly concerning sensitive data such as personal identifiers and financial information. In contrast, Amazon users exhibited knowledge gaps despite reporting higher self-perceived privacy awareness in prior studies. These findings suggest that privacy literacy is culturally influenced and that procedural privacy behaviors may not align with knowledge in high power distance societies. The study emphasizes the need for platform-specific privacy education and culturally informed approaches to support informed privacy decisions online.

Keywords: privacy literacy; declarative knowledge; e-commerce platforms; data collection practices; cross-cultural privacy comparison; privacy regulations

Introduction

The privacy paradox refers to the phenomenon where individuals express privacy concerns but fail to engage in corresponding protective behaviors online (Acquisti & Gross, 2006; Baruh et al., 2017; King et al., 2011; Kumar, 2023; Petina et al., 2016). This paradox is widely observed in digital environments, raising questions about its underlying causes. One key factor is the complexity of privacy policies, which require significant time and literacy to comprehend (McDonald et al., 2009). Additionally, many individuals lack the necessary knowledge to translate privacy concerns into protective behaviors. Studies indicate that limited knowledge, specifically low privacy literacy, prevents users from acting in line with their concerns, emphasizing privacy literacy's role in shaping behavior (Park, 2011; Trepte et al., 2014; Veghes et al., 2012; Weinberger et al., 2017; Wissinger, 2017).

Privacy literacy encompasses both declarative knowledge (understanding data collection practices, privacy laws, and risks) and procedural knowledge (practical skills such as managing settings and applying privacy protection tools) (Prince et al., 2023; Trepte et al., 2015). However, prior research suggests that individuals frequently underestimate the visibility of their personal data, limiting their ability to adopt protective measures (Choi, 2022; Ma & Chen, 2023; Park, 2011; Prince et al., 2023). Moreover, much of the existing research relies on self-reported awareness rather than empirically testing users' actual understanding. This gap is particularly notable regarding users' knowledge of corporate data practices—what data is collected, how it is used, and for what purposes.

This study focuses on investigating users' declarative privacy knowledge, specifically their understanding of platform data collection practices in cross-cultural e-commerce environments, in the United States and China in particular. Privacy literacy is dynamic and shaped not only by evolving regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Personal Information Protection Law (PIPL) in China, but also by societal discourse, media coverage, and high-profile data breaches (Hua & Wang, 2025; Meier & Krämer, 2024). Given that the United States lacks a national privacy law, this study also explores cross-cultural differences in privacy literacy to understand how different regulatory and social environments influence users' declarative knowledge. By empirically testing users' understanding of platform data practices, this study aims to bridge the gap between perceived and actual privacy literacy in e-commerce. The findings will contribute to ongoing discussions about privacy education and policy design, ultimately supporting better-informed privacy decisions in digital ecosystems. This study addresses the following research question: To what extent do users in different cultural contexts demonstrate correct knowledge of e-commerce platforms' data collection practices?

Literature Review

Defining Privacy Literacy

Privacy literacy broadly refers to an individual's knowledge, awareness, and skills necessary to manage personal data and privacy risks online (Park, 2011; Trepte et al., 2014; Veghes et al., 2012; Wissinger, 2017). Scholars conceptualize privacy literacy as comprising two core components: declarative knowledge—understanding institutional data practices, privacy risks, regulations—and procedural knowledge, or the ability to apply practical skills such as managing privacy settings and using protective technologies (Nguyen et al.,2024; Prince et al., 2023; Trepte et al., 2015).

Table 1 presents key definitions of privacy literacy from existing literature, illustrating how the concept has evolved to encompass technical knowledge, institutional practices, and data protection mechanisms.

Table1. Key definitions of privacy literacy

Study	Privacy literacy Scope
Park (2011)	Digital privacy literacy consists of three dimensions: technical familiarity, awareness of institutional practices, and policy understanding. It includes both declarative and procedural knowledge.
Trept et al. (2015)	Privacy literacy consists of five dimensions: knowledge of institutional practices, technical knowledge, awareness of risks, legal knowledge, and privacy strategies. Includes both declarative and procedural components.
Rakhmanov (2021)	Privacy literacy is the knowledge of how data is collected and techniques to prevent data collection.
Prince et al. (2023)	Privacy literacy consists of two main dimensions: (1) declarative knowledge (laws, policies, risks) and (2) procedural knowledge (practical skills for privacy protection).
Meier & Krämer (2024)	Privacy literacy is defined as factual knowledge about online privacy and data protection, including understanding data collection, usage, risks, and protection mechanisms.

Prior studies also suggest that users often overestimate their knowledge, particularly regarding organizational data practices (Ma & Chen, 2023; Park, 2011). Therefore, while privacy literacy spans multiple areas, this study focuses specifically on declarative knowledge of platform data practices—a critical yet often overlooked component in empirical assessments, essential for evaluating privacy risks and making informed decisions.

Measuring Declarative Privacy Literacy: Existing Studies and Limitations

Declarative knowledge is foundational for assessing privacy risks and making informed privacy decisions (Park, 2011; Barth et al., 2022). However, prior research has primarily focused on general knowledge of privacy laws, risks, or technical familiarity while paying less attention to users' understanding of specific organizational data practices. Table 2 summarizes existing studies that attempted to measure declarative privacy literacy and identifies key limitations.

Table 2: Prior Studies Assessing Declarative Privacy Literacy and Limitations

Study	Findings	Limitations
Park (2011)	Explored user knowledge and digital literacy across general internet users. Found technical familiarity improved control of settings but not understanding of surveillance or policies.	Used yes/no questions, focused on general users, not platform-specific literacy.
Trepte et al. (2015)	Developed OPLIS scale using factual test items focused on legal frameworks and privacy policies.	Emphasized conceptual legal knowledge; limited attention to data practice knowledge.
Prince et al. (2023)	Measured declarative knowledge of laws and rights. Acknowledged self-report biases.	Did not measure corporate data practices; relied on true/false and self-reporting.
Ma & Chen (2023)	Assessed subjective and objective privacy literacy, highlighting gaps between perceived and actual knowledge.	Focused on general technological familiarity, not organizational data practices.
Meier & Krämer (2024)	Measured general factual knowledge via quiz questions about privacy risks and protection mechanisms.	Did not assess specific platform data practices or organizational data flows.

Before turning to Table 2, it is important to acknowledge that several studies have attempted to measure declarative privacy literacy using different approaches and frameworks. These studies primarily focus on general digital literacy, privacy risks, or legal frameworks and do not specifically assess users' knowledge of e-commerce platform data practices. Most rely on self-reported knowledge, which has been criticized for overestimating users' actual understanding, as individuals often misjudge their knowledge of organizational data practices (Ma & Chen, 2023; Park, 2011; Prince et al., 2023). Even objective-looking formats like true/false quizzes fall short, as users may guess when uncertain, masking knowledge gaps. As a result, these methods struggle to accurately capture users' declarative knowledge about how organizations collect and use data—knowledge essential for evaluating privacy risks in platform-specific contexts.

The Need to Focus on Platform Data Practices

Understanding platform-specific data practices is crucial for privacy literacy, particularly in e-commerce contexts where data collection is highly context-dependent (Barth et al., 2022; Nguyen et al., 2024). According to Barth et al. (2022), platform data collection practices vary across contexts, meaning that knowledge about one platform's data practices may not transfer to another. This highlights the importance of assessing users' understanding of specific organizational data practices rather than general privacy knowledge. Users cannot accurately assess privacy risks or make informed decisions without knowing what data is collected and how it is used. While technical familiarity helps users adjust settings, it does not necessarily improve awareness of corporate data practices or privacy policies (Park, 2011; Kumar, 2023).

Declarative knowledge about data collection practices serves as the foundation for privacy-related decisions (Barth et al., 2022; Meier & Kramer, 2024; Nguyen et al., 2024; Park, 2011; Prince et al., 2023; Rakhmanov, 2021; Wissinger et al., 2017). Without this knowledge, even technically skilled users may underestimate risks or make choices based on misconceptions. Recent research emphasizes that being tech-savvy does not equate to being privacy-savvy (Park, 2011; Prince et al., 2023). Users need not only procedural skills but also a clear understanding of how platforms collect, process, and use their personal data.

Cultural frameworks further complicate privacy understanding and behavior

Numerous studies underscore that privacy is not a universally defined concept, but rather one shaped by cultural norms, regulatory expectations, and orientations toward collectivism versus individualism (Acquisti et al., 2016; Hofstede, 2001; Lukács, 2016; Milberg et al., 2000). In collectivist cultures such as China, personal data sharing may be viewed as a means of fostering communal benefit or as an expression of trust in institutional oversight. In contrast, individuals in more individualistic societies like the United States often place greater emphasis on personal autonomy and control over information flows (Hua & Wang, 2023). These cultural dimensions influence how users evaluate the risks of data disclosure and the significance they assign to privacy rights. As such, cross-cultural differences are not merely contextual but fundamentally shape privacy-related attitudes and decision-making. Accordingly, they must be accounted for in any empirical evaluation of privacy literacy.

Literature Gap and Study Contribution

In summary, while prior studies offer valuable frameworks for conceptualizing privacy literacy, few empirically assess users' knowledge of platform-specific data practices in e-commerce contexts. Most existing studies prioritize legal and technical knowledge, often relying on self-reports that overestimate actual knowledge levels (Ma & Chen, 2023; Prince et al., 2023). This study addresses this gap by testing users' factual knowledge of data collection practices on e-commerce platforms and examining cross-cultural differences. Findings aim to inform privacy education and policy design, promoting more informed online privacy decisions.

Methodology

This study evaluates users' awareness of data collection practices employed by e-commerce platforms, focusing on Amazon in the U.S. and Taobao in China. Unlike prior research that often relied on self-reported privacy awareness—which may overestimate actual knowledge levels—this study employs an objective, knowledge-based assessment to measure users' declarative knowledge. To contextualize the development of the survey instrument, a comparison was made between the surveillance awareness questions from Park (2011) and the e-commerce privacy literacy questions formulated for this study. This comparison highlights the shift from general online surveillance topics to specific data collection practices pertinent to e-commerce platforms. Table 3 presents this comparative analysis.

Table 3: Comparison of Park (2011) and Current Study's Privacy Literacy Questions

No.	Park (2011) – Surveillance Awareness Questions	Current Study – E-Commerce Privacy Literacy Questions (Amazon & Taobao)	Common Theme
1	When you visit a website, it can collect information about you even if you do not register.	Internet Protocol (IP) address	Passive data tracking (IP, cookies)

No.	Park (2011) – Surveillance Awareness Questions	Current Study – E-Commerce Privacy Literacy Questions (Amazon & Taobao)	Common Theme
2	Popular search engine sites, such as Google, track the sites you come from and go to.	Full Uniform Resource Locator (URL) clickstream	Search behavior tracking (clickstream)
3	E-commerce sites, such as Amazon or Netflix, may exchange your personal information with law enforcement and credit bureaus.	Credit history information, corporate and financial information, identity documents (e.g., Social Security, driver's license)	Institutional data sharing (financial & identity data)
4	What a computer user clicks while online surfing can be recorded as a trail.	Content interaction information (downloads, streams, playback details)	Clickstream & behavioral tracking
5	Most online merchants monitor and record your browsing on their sites.	Purchase and content use history, phone numbers used to call customer service	User behavior tracking
6	When a website has a privacy policy, it means the site will not share your information with other websites or companies.	Not directly tested	Privacy policy misconceptions
7	U.S. government agencies can collect information about you online without your knowledge and consent.	Credit history information, corporate and financial information, identity documents (Social Security, driver's license).	Government surveillance
8	A website is legally allowed to share information about you with affiliates without telling you the names of the affiliates.	Amazon Services metrics, device metrics, and settings preferences	Third-party data sharing (system performance & user settings)
9	Not included in Park's study	Name, address, phone number, payment info, email, personal profile data, images, voice recordings, and location	Personal identifiers & biometric data collection

To provide a structured overview of the specific data types assessed in this study, Table 4 categorizes the data collection practices of e-commerce platforms into distinct categories, including Personally Identifiable Information (PII) and Behavioral Data.

Table 4: Categorization of Data Collection Practices in E-Commerce Platforms

Data Category	Examples of Data Types	Description
Personally Identifiable Information (PII)	Name, Address, Phone Number, Payment Information, Email Address	Direct identifiers, financial data, and contact information used to identify or communicate with individuals.
Behavioral Data	Purchase History, Clickstream Data, Content Interaction Information	Records of user behavior, such as purchases, site navigation, page views, downloads, and streaming activities.
Device Information	IP Address, Device Metrics	Technical data about users' devices, including network identifiers, operating systems, and browser types.
Biometric Data	Voice Recordings	Audio data collected through voice-enabled features.

Survey Design

To mitigate the limitations associated with binary (yes/no) questions, which can lead to guessing and fail to capture the nuances of users' understanding, this study utilizes a 5-point Likert scale. Participants indicate the likelihood that each data type is collected by the platform, ranging from "Least Likely" (1) to "Most Likely" (5). This approach reduces the impact of random guessing and captures nuanced user perceptions.

Data Collection

Data were collected from Amazon users in the U.S. and Taobao users in China between July and September 2024. The study received approval from the Institutional Review Board (IRB), ensuring adherence to ethical research standards. A total of 318 valid responses were collected from Amazon users through CloudResearch, and 189 valid responses were collected from Taobao users through WeChat. Participants were recruited based on their experience using either Amazon or Taobao to ensure platform familiarity. Basic demographic information, including age and gender, was collected to describe the sample and assess representativeness.

While demographic information was available for 199 Taobao participants, only 189 responses were valid and complete for the knowledge-based survey questions. Therefore, analyses were conducted based on the 189 valid responses. The demographic data reported in Table 5 reflect the broader sample but may slightly differ from the final analytical sample.

Table 5: Demographic Characteristics of Respondents on Amazon and Taobao Platforms

Demographic Variable	Category	Amazon (n=318)	Amazon (%)	Taobao (n=199)	Taobao (%)
Gender	**Female**	141	44.3	99	49.7
	Male	172	54.1	73	36.7
	Non-traditional	2	0.6	-	-
	Not willing to say	1	0.3	3	1.5
	No answer provided	2	0.6	24	12.1
Age Range	**18–24**	28	8.8	19	9.5
	25–34	118	37.1	37	18.6
	35–44	104	32.7	47	23.6
	45–54	40	12.6	40	20.1
	55–64	19	6	28	14.1
	65+	7	2.2	4	2
	No answer provided	2	0.6	24	12.1

Data Preparation, Coding, and Analysis

In the data preparation phase, responses were coded to address potential biases from random guessing. Only responses marked as "Most Likely" (5) were coded as correct, while all other responses (1–4) were coded as incorrect. This stringent criterion ensured that only confident assessments were considered correct, enhancing the reliability of the measured knowledge. To compare awareness levels between Amazon and Taobao users, chi-square tests were conducted to examine differences in correct identification of platform data collection practices. Statistical significance was set at $p < .05$ for all tests.

Results

This study assessed users' declarative knowledge of platform-specific data collection practices across four data categories: Personally Identifiable Information (PII), Behavioral Data, Device Information, and Biometric Data. Chi-square tests were conducted to compare Amazon and Taobao users' accuracy in identifying whether specific types of data were collected by the platform (see Table 6).

Table 6: Descriptive Statistics and Chi-Square Results Comparing Amazon and Taobao Users' Declarative Knowledge of Data Collection Practices by Data Category

Data Category	Data Type	Amazon Correct (%)	Taobao Correct (%)	χ^2(df)	*p*-value	Better Performing Platform	Significance
PII	Name	53.80%	61.40%	2.79 (1)	0.095	Taobao	ns
	Home Address	45.60%	62.40%	13.46 (1)	<.001	Taobao	***
	Personal Phone Number	33.60%	76.70%	87.97 (1)	<.001	Taobao (large gap)	***
	Payment Information	36.50%	60.80%	28.38 (1)	<.001	Taobao	***
	Age	48.40%	45.00%	0.57 (1)	0.451	Amazon (slightly)	ns
	Email Address	44.70%	43.90%	0.03 (1)	0.871	Amazon (neg ligible)	ns
	Identity Number	13.90%	53.00%	88.01 (1)	<.001	Taobao (large gap)	***
	Corporate Financial Information	14.20%	34.10%	27.10 (1)	<.001	Taobao	***
	Credit History	13.90%	50.50%	78.41 (1)	<.001	Taobao (large gap)	***
Behavioral Data	Review Content & Emails	39.90%	44.90%	1.17 (1)	0.28	Taobao	ns
	Uploaded Images/Videos	26.50%	49.20%	26.49 (1)	<.001	Taobao	***
	Content Interaction Information	46.40%	44.00%	0.27 (1)	0.602	Amazon (slightly)	ns
	Platform Service Metrics	56.50%	59.90%	0.56 (1)	0.456	Taobao (small)	ns
	Purchase & Content History	68.50%	72.50%	0.91 (1)	0.339	Taobao (small)	ns
	URL Click Stream	30.60%	65.40%	56.99 (1)	<.001	Taobao (large gap)	***
	Phone Call to Customer Service	29.70%	52.20%	24.98 (1)	<.001	Taobao	***
	Images/Photos During Shopping	20.20%	50.00%	47.98 (1)	<.001	Taobao (large gap)	***

Data Category	Data Type	Amazon Correct (%)	Taobao Correct (%)	χ²(df)	*p*-value	Better Performing Platform	Significance
Device Information	Device Location	47.90%	43.40%	0.96 (1)	0.327	Amazon (slightly)	ns
	Device Metrics	50.20%	42.30%	2.86 (1)	0.091	Amazon (slightly)	ns
Biometric Data	Voice Recording	21.80%	34.60%	9.87 (1)	0.002	Taobao	**

Personally Identifiable Information (PII)

Significant differences were found in most PII items, with Taobao users performing better on recognizing data collection practices. Specifically, Taobao users were significantly more accurate in identifying the collection of home addresses ($\chi^2(1) = 13.46$, $p < .001$), personal phone numbers ($\chi^2(1) = 87.97$, $p < .001$), payment information ($\chi^2(1) = 28.38$, $p < .001$), identity numbers ($\chi^2(1) = 88.01$, $p < .001$), corporate financial information ($\chi^2(1) = 27.10$, $p < .001$), and credit history ($\chi^2(1) = 78.41$, $p < .001$).For name, age, and email address, no significant differences were observed ($p > .05$).

Behavioral Data

Taobao users also outperformed Amazon users in several behavioral data types. Significant group differences were found for uploaded images/videos ($\chi^2(1) = 26.49$, $p < .001$), URL clickstream data ($\chi^2(1) = 56.99$, p < .001), phone call records to customer service ($\chi^2(1) = 24.98$, p < .001), and images/photos during shopping ($\chi^2(1) = 47.98$, $p < .001$) — with Taobao users demonstrating higher accuracy. No significant differences emerged for review content and emails, content interaction information, platform service metrics, or purchase and content history ($p > .05$).

Device Information

There were no significant differences between Amazon and Taobao users regarding device-related data. Both groups showed similar recognition rates for device location (p = .327) and device metrics ($p = .091$).

Biometric Data

For voice recordings, Taobao users demonstrated significantly better knowledge than Amazon users ($\chi^2(1) = 9.87$, $p = .002$).

Discussion

This study found significant cross-platform differences in users' declarative knowledge of data collection practices, particularly regarding personally identifiable information (PII) and behavioral data. Taobao users consistently outperformed Amazon users in recognizing specific data types collected by the platform.

Technical familiarity does not equate to privacy literacy

These findings are consistent with Park (2011), who argued that users often lack awareness of how organizations collect and process personal data. In line with Park's observation that technical familiarity does not equate to privacy literacy, it was found that even experienced e-commerce users struggled to recognize platform-specific data practices—particularly Amazon users. Notably, an unpublished dissertation by Hua (2025) reported that Amazon users perceived themselves as significantly more aware of privacy choices, performed better in comprehension tests of privacy-related information, and were more successful in completing privacy decision tasks. This reflects greater familiarity with privacy policies and procedural knowledge for protecting online privacy. However, when factual knowledge of organizational data collection practices was assessed, Taobao users were found to possess stronger declarative knowledge of privacy literacy compared to Amazon users.

Furthermore, Park (2011) noted that self-reported privacy concerns often overestimate actual knowledge—a pattern that was also observed in this study. To address this limitation, our study employed a five-point Likert scale to measure users' factual knowledge, allowing respondents to indicate their confidence levels rather than relying solely on binary answers. This approach helped mitigate random guessing and offered a more nuanced, objective assessment of declarative knowledge. Although Amazon users rated themselves as more privacy-aware, factual knowledge testing revealed substantial gaps, particularly regarding sensitive data types such as credit history and personal identifiers.

Cultural Influence on Privacy Protection Behaviors

While Taobao users demonstrated better declarative knowledge of platform data practices, this knowledge does not necessarily translate into privacy-protective behaviors or heightened privacy concerns. Declarative knowledge is assumed to enable individuals to assess risks more accurately, which should, in theory, lead to greater protective behaviors. However, based on the author's prior study (Hua, 2025, unpublished dissertation), Taobao users reported greater trust in platforms compared to Amazon users, despite expressing significantly lower satisfaction with price-related features provided by the platforms.

These findings align with the Cross-Cultural Privacy Model proposed by Hua and Wang (2023), which suggests that in high power distance and collectivist cultures, such as China, individuals are more likely to trust large organizations or authorities even when they are aware of extensive data collection practices. This cultural dynamic may reduce users' motivation to engage in procedural privacy protection behaviors, despite their awareness of organizational data practices. As a result, Taobao users may feel less necessity or personal agency to act on their knowledge, which could explain the gap between declarative knowledge and protective behavior.

This observation raises an important question: Should cultural factors be incorporated into the conceptualization of privacy literacy? Specifically, if procedural knowledge is assumed to be universally required for privacy protection, cultural variations may challenge this assumption. Prior research generally argues that declarative knowledge is positively associated with privacy concerns and protective behavior (Barth et al., 2022; Trepte et al., 2015). However, our findings suggest that this relationship might be culturally dependent, requiring a more nuanced understanding of privacy literacy in cross-cultural contexts.

Do Privacy Regulations Shape Declarative Knowledge?

Unlike prior studies that focused on general knowledge of privacy laws or technical familiarity (Prince et al., 2023; Meier & Krämer, 2024), this study tested users' knowledge of actual platform data collection practices—an often overlooked but critical component of privacy literacy. The significant gaps identified align with Meier and Krämer (2024), who found that users tend to overestimate their knowledge of digital data practices. Interestingly, our cross-cultural comparison further extends these findings by showing that regulatory and cultural contexts, such as the presence of China's Personal Information Protection Law (PIPL), may contribute to enhancing user knowledge on platforms like Taobao.

This raises important questions about the potential role of privacy regulations in shaping public awareness: Does the existence of comprehensive privacy laws like PIPL increase users' factual knowledge of organizational data practices? Or do other factors, such as media discourse, platform communication strategies, or cultural attitudes toward data collection, also influence users' knowledge? Future research is needed to disentangle the specific influence of regulatory environments from other contextual factors in shaping privacy literacy across different platforms and regions.

Conclusion

This study extends prior research on privacy literacy by moving beyond general privacy awareness to examine users' declarative knowledge of organizational data practices within specific e-commerce platforms. By focusing on Amazon and Taobao, the study highlights that users' understanding of what data is collected by platforms remains limited—particularly among Amazon users—even as privacy discourse and regulations have evolved. Building on Park (2011), who explored general surveillance awareness prior to major privacy regulations, this study provides a platform-specific perspective in the current regulatory landscape shaped by the GDPR and PIPL. The findings suggest that while regulations may influence knowledge in certain contexts, significant gaps persist, especially regarding sensitive personal data.

Importantly, this research also strengthens methodological approaches in privacy literacy studies. A five-point Likert scale was employed to assess users' knowledge objectively, moving beyond self-reported awareness or binary response formats. This design allowed for a more nuanced measurement of users' confidence in their knowledge and helped mitigate random guessing—offering a more reliable assessment of declarative privacy literacy.

Importantly, this research demonstrates the need for platform-specific privacy education. General digital literacy or technical familiarity does not guarantee accurate understanding of platform data practices. This is especially evident for Amazon users, who reported higher self-perceived privacy awareness (Hua, 2025) but showed lower factual knowledge compared to Taobao users. Furthermore, cultural factors—such as high-power distance and collectivism—may shape how users in different regions translate knowledge into privacy-protective behaviors, raising critical questions about the cultural dependency of procedural privacy literacy.

Several limitations should be acknowledged. This study relied on self-reported familiarity with platforms and may not fully capture actual user engagement or experience. Additionally, the cross-sectional design cannot establish causality between regulatory environments and knowledge levels. Future research should explore how platform design, cultural norms, and media discourse jointly influence both declarative and procedural privacy literacy. Longitudinal studies could also assess how privacy knowledge evolves over time, especially in response to regulatory changes or high-profile data breaches.

Overall, this study underscores the importance of integrating platform-specific and culturally sensitive approaches into privacy literacy research and education. Privacy literacy is not universal, and improving it requires targeted strategies that empower users to make informed privacy decisions in diverse digital environments. The findings provide actionable insights for platform designers and privacy professionals. Identifying users' knowledge gaps—especially among U.S.-based users—can inform the development of clearer, culturally tailored privacy notices and interface controls. Practitioners can apply these results to enhance transparency and foster trust through simplified, localized communication strategies.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. Journal of Economic.

Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer, Berlin, Heidelberg.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Choi, S. (2022). Privacy literacy on social media: Its predictors and outcomes. *International Journal of Human–Computer Interaction*, *39*(1), 217–232. https://doi.org/10.1080/10447318.2022.2041892

Hua, J., & Wang, P. (in press). Security or privacy? A cross-cultural exploration of consumer priorities in e-commerce. *International Conference on Information Technology: New Generations (ITNG 2025)*. Springer

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is there an app for that? *Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11*. https://doi.org/10.1145/2078827.2078843

Kumar, P. C. (2023). Orienting privacy literacy toward social change. *Information and Learning Sciences*, *125*(5/6), 346-366.

Lukács, A. (2016). What is privacy? The history and definition of privacy.

Ma, R., & Chen, J. (2023). Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior. *Frontiers in Psychology, 14*,1224168. https://doi.org/10.3389/fpsyg.2023.1224168

McDonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009, August). A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies Symposium* (pp. 37-55). Springer, Berlin, Heidelberg.

Meier, Y., & Krämer, N. C. (2024). Differences in access to privacy information can partly explain digital inequalities in privacy literacy and self-efficacy. *Behaviour & Information Technology*, 1–16. https://doi.org/10.1080/0144929x.2024.2349183

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization science, 11*(1), 35-57.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research, 40(*2), 215–236. https://doi.org/10.1177/0093650211418338

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2014). Do people know about privacy and data protection strategies? Towards the “online privacy literacy scale” (OPLIS). *Law, Governance and Technology Series*, 333–365. https://doi.org/10.1007/978-94-017-9385-8_14

Veghes, C., Orzan, M., Acatrinei, C., & Dugulan, D. (2012). Privacy literacy: what is and how it can be measured? *Annales Universitatis Apulensis: Series Oeconomica*, *14*(2), 704.

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review*, *41*(5), 655-671.

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy*, *11*(2), 378-389.