doi: 10.29843/JCCIS.202507_(49).0002

行動商務中的隱私計算：行動隱私知識與技能的調節作用

呂卓勳

摘要

智慧感測器與人工智慧透過分析使用者的數位足跡，提升了行動商務的效能。本研究針對 423 名台灣受訪者的研究，運用隱私計算理論，探討了影響隱私顧慮與對行動服務信任的效益與風險。研究結果顯示，感知效益與風險顯著影響隱私顧慮與信任。並且行動隱私知識與技能均調節了隱私顧慮與資訊揭露意圖之間的關係。行動隱私技能則調節信任與資訊揭露意圖的關係，但在知識對資訊揭露意圖之間的調節效果則呈現統計不顯著。本研究提供了一個整合模型，幫助行動服務提供商理解使用者的資訊揭露意圖。

⊙ **關鍵字：隱私悖論、隱私計算、行動隱私知識、行動隱私技能、移動商務、隱私素養**

⊙ **本文作者呂卓勳為元智大學工業工程與管理學系助理教授。**

⊙ **聯絡方式：Email：chohsunlu@saturn.yzu.edu.tw；通訊處：桃園市中壢區遠東路135號元智大學工業工程與管理學系。**

⊙ **收稿日期：2025/02/05　接受日期：2025/07/24**

Exploring Privacy Calculus in Mobile Commerce: Moderating Effect of Mobile Privacy Knowledge and Skills

Cho-Hsun Lu

Abstract

Intelligent sensors and AI have enhanced mobile commerce by analyzing users' digital footprints. Using privacy calculus theory, a study of 423 Taiwanese respondents examined the benefits and risks impacting privacy concerns and trust in mobile services. Findings revealed that perceived benefits and risks significantly affect privacy concerns and trust. Mobile privacy knowledge and skills moderate the relationship between privacy concerns and disclosure intention. Mobile privacy skills moderate trust and disclosure intention, while knowledge does not. This study offers an integrated model to help mobile service providers understand users' intentions to disclose information.

⊙ Keywords: Privacy Paradox, Privacy Calculus, Mobile Privacy Knowledge, Mobile Privacy Skills, Mobile Commerce, Privacy Literacy

⊙ The author, Cho-Hsun Lu, is an assistant professor from the Department of Industrial Engineering and Management at Yuan Ze University.

⊙ Corresponding author: Cho-Hsun Lu, email: chohsunlu@saturn.yzu.edu.tw; address: Department of Industrial Engineering and Management, Yuan Ze University, No135, Yuandong Rd., Zhongli Dist., Taoyuan City 320315, Taiwan

⊙ Received: 2025/02/05 Accepted: 2025/07/24

Introduction

Wireless communication technology has significantly influenced the evolution of e-commerce, expanding business operations beyond traditional websites to include smartphones and other mobile devices, a phenomenon termed mobile commerce. Mobile commerce distinguishes itself by offering a ubiquity feature that has become increasingly prevalent over the past decade. Furthermore, modern mobile commerce is characterized by its ability to provide instantaneous, ubiquitous, localized, and personalized services tailored to individual user attributes, offering a marked advancement over conventional e-commerce (Wang et al., 2015). In contrast to conventional e-commerce platforms, integrating context awareness enabled by mobile device sensors promotes innovative service delivery by utilizing user location and behavioral trail. However, this advancement brings privacy issues stemming from the gathering and using of data for tailored services and targeted advertising purposes (Mollah et al., 2017). In addition, the capability to collect, aggregate, and analyze an individual's digital identity using big data and AI algorithms, thereby creating detailed digital footprints or profiles, exacerbates these concerns (Eastin et al., 2016; Ge et al., 2022). Thus, advanced intelligent sensors and data analytics technologies, such as big data and AI algorithms, have enabled mobile service providers to offer personalized mobile commerce services based on the analysis of consumer digital trails (Eastin et al., 2016; Fox et al., 2021). The reliance on user identification and behavior analysis for mobile services is accompanied by privacy and security challenges, potentially fostering a reluctance toward mobile commerce (Balapour et al., 2020; Sarker et al., 2021; Shaw & Sergueeva, 2019). New mobile technologies enhance service convenience but also necessitate increased information disclosure from consumers, leading to heightened privacy and security concerns (Balapour et al., 2020). This concern is evidenced by worries about sharing personal information in return for the convenience and personalization offered by mobile services (Degirmenci, 2020).

The public has noted security and privacy concerns for mobile apps' private content (e.g., personal passwords, location history, photos, and contacts). Mobile devices can easily

collect and analyze user data, health application logs, geolocation data, and various other types of information. People perceive significant threats because third parties could track and misuse their personal information. Past research has examined Internet users' perceptions and behaviors in privacy decisions and found that despite concerns that their privacy may be violated, users are inclined to give out their data to access online services (Chen & Chen, 2015; Trepte et al., 2015). The "privacy paradox" can be attributed to the inconsistency in privacy-related behavior observed in online and mobile environments (Barth & de Jong, 2017). This inconsistency indicates that information privacy concerns of individuals do not consistently predict the privacy behavior of disclosure (Baruh et al., 2017). Some researchers suggest the "privacy calculus theory" to explain the discrepancy between online service users' privacy concerns and their actual behavior regarding the disclosure of private information (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Consumers evaluate the trade-off between the pros and cons of self-disclosure and determine final behavior by the relative significance of advantages and concerns (Dinev & Hart, 2006).

The privacy calculus theory posits that disclosing information is a rational and calculated decision, implying that one's choice to disclose private information is predominantly shaped by evaluating its potential advantages and disadvantages (Culnan & Armstrong, 1999; Dinev & Hart, 2006). This approach underscores the rationality behind personal information-disclosure choices. However, empirical studies by Barth & de Jong (2017) and Kokolakis (2017) indicate that the decision-making process in privacy disclosure is often hindered by incomplete information, bounded rationality, and cognitive biases. Information disclosure behavior encompasses not solely an individual's rational evaluation of associated risks and benefits, but is also affected by situational factors, which lead to differences in individuals' behaviors of disclosing personal information. Since situational factors may lead to privacy paradox, the present study is based on the research conducted by Park and Mo Jang (2014) and Trepte et al. (2015), individual differences in privacy knowledge and skills required to 5j03rul3manage personal data on online and mobile platforms effectively are contextual factors, the concept of "privacy literacy," exploring the

differences between individuals' attitudes towards privacy and actual behaviors of privacy protection. Park & Mo Jang (2014) highlight the importance of adequate knowledge and skills for mobile privacy issues. Differences in privacy awareness and protective skills may explain gaps between people's privacy attitudes and behaviors (Trepte et al., 2015). For example, many users incorrectly believe that their private data is undoubtedly protected and managed in the legal process. In addition, low online privacy literacy revealed technical familiarity, such as the ability to control private and location data usage on mobile phones. Recent efforts in privacy studies have investigated personal data protection knowledge and skills in online and mobile environments. People inevitably provide personal data to other companies or organizations to access mobile services. Therefore, information and locational privacy knowledge and skills become critical "mobile privacy literacy" for wireless service users (Park & Mo Jang, 2014).

In mobile commerce, the exchange of private personal information is prevalent and deemed indispensable. Mobile apps exhibit a state of being "context-aware," whereby the sensors integrated within mobile devices readily gather personal information and data trails (Almusaylim & Jhanjhi, 2020; Sarker et al., 2021). Subsequently, personal data are subjected to processing through big data and AI algorithms, facilitating tailored mobile services (Sarker et al., 2021). However, the public often lacks awareness of data collection and privacy issues, hindering their ability to manage personal information on mobile services. Park and Mo Jang (2014) suggest that in an era where mobile services are ubiquitous, addressing privacy concerns becomes an indispensable skill for users. We propose extending the privacy calculus theory by considering privacy knowledge and skills as contextual factors. This extension explores users' decision-making process when disclosing personal information in mobile environments and the role of privacy literacy.

This study employed the privacy calculus theory to understand consumers' decisions regarding private information disclosure in mobile commerce. Furthermore, we attempt to understand how mobile privacy skills and knowledge are associated with the privacy paradox in mobile commerce. Firstly, the demand for mobile service providers to collect, aggregate,

and analyze consumer data to offer innovative and intelligent services is consistently rising (Mollah et al., 2017). Nonetheless, users often lack the knowledge and skills to make well-considered decisions regarding disclosing personal privacy information (Sarkar et al., 2020). The present study argues that privacy knowledge and skills play a direct and moderating role in weighing the benefits and risks of information disclosure. Moreover, previous research has indicated that disparities in individuals' comprehension of privacy knowledge and capacity to manage personal data can influence their attitudes toward information privacy and subsequent actions. (Desimpelaere et al., 2020; Masur, 2020). Consequently, we posit that investigating this phenomenon through the lens of privacy knowledge and skills can offer a more profound comprehension of the privacy paradox.

This research explores the relationship between perceived risks and benefits in mobile commerce and its consequential influence on assessing information privacy concerns and trust. Additionally, the present study investigates the potential moderating effect of mobile privacy skills and knowledge in providing mobile commerce services. Our primary objective is to understand how privacy calculus principles are intertwined with the moderating effects of mobile privacy skills and knowledge. This exploration is undertaken to shed light on the disparities that may arise in individuals' intentions to disclose personal information within mobile commerce. Therefore, our investigation diverges from prior research by emphasizing the crucial significance of users' capacity to control privacy information, which might influence their decision-making procedures within mobile commerce. Considering these research gaps, this study aims to explore and investigate the following research objectives:

1. Examine how perceived benefits and risks of users impact their privacy concerns and trust in mobile commerce platforms.

2. Determine how privacy concerns and trust of users affect their willingness to disclose information in mobile commerce.

3. To investigate the moderation effect of mobile privacy knowledge and skills in relationships between privacy concerns, trust, and intention to disclose information in mobile commerce contexts.

Literature Review

Mobile commerce information privacy issues

The pervasive adoption of mobile commerce among consumers can be attributed to its ubiquitous accessibility and convenience, enabling access to information and services anytime and anywhere (Sarkar et al., 2020; Wang et al., 2015). Furthermore, mobile commerce can provide personalized services using precise technologies such as data mining, collaboration technology, usage patterns, location detection, transaction history, and AI algorithms (Kang & Namkung, 2019; Luo et al., 2023; Zhang et al., 2023). Personalized services help consumers save time by providing tailored information and customized services to meet their needs better (Zhang et al., 2023). For businesses, personalization is a crucial consumer relationship marketing strategy (Martins et al., 2019).

Notwithstanding these advantages, the pervasiveness of mobile commerce has given rise to concerns regarding information security and privacy issues (Balapour et al., 2020; Kang & Namkung, 2019). In the same way as e-commerce services, mobile applications are susceptible to multiple security uncertainties and risks, including phishing, malicious software, cyberattacks, and unsafe network services (He et al., 2015). Coupled with the widespread application of mobile technology, the rapid development of data mining and AI algorithms has promoted innovations in mobile services, ultimately offering intelligent and customized services (Hoehle et al., 2012; Siyal et al., 2024; Wang et al., 2023). In contrast to previous e-commerce services, consumers engaging in mobile commerce express heightened concerns regarding the extensive gathering, deliberate and inadvertent disclosure, and misuse of personal information (Eastin & Brinson, 2017; Eastin et al., 2016).

Among these vulnerabilities, the ability of mobile devices to track user identities has significantly broadened the scope of privacy issues in e-commerce, exhibiting a notable distinction from traditional stationary e-commerce, particularly in data collection and analytics techniques (Sarker et al., 2021; Zhang et al., 2013). Mobile devices carried by individuals or in their pockets can collect personal information, such as financial details,

societal background, biological metrics, and spatial tracking (Ho et al., 2023). In addition, the advanced data collection features of mobile devices, coupled with the extensive integration of data mining (Eastin & Brinson, 2017; Eastin et al., 2016) and AI algorithms (Sarker et al., 2021; Zhang et al., 2023), facilitate the rapid and comprehensive acquisition, analysis, and synthesis of users' data. Unlike online services tied to specific locations and depending on wired networks, e-commerce on mobile networks affords ubiquitous accessibility. The evolution of data science technologies has empowered service providers to analyze consumers' usage behavior, personal preferences, historical usage patterns, and social network data on online and mobile platforms, facilitating the development of personalized usage profiles (Khemiri & Jallouli, 2022). Thus, privacy issues transcend mere data collection to encompass broader dimensions such as data misuse, identity theft, and lack of transparency (Sarker et al., 2021).

The physical business services and e-commerce sector have been significantly influenced by the COVID-19 pandemic since late 2019, leading to a shift towards unmanned and mobile services. In response to the growing emphasis on health and safety, public health systems worldwide have implemented contact tracing apps to monitor the movements and interactions of individuals (Cho et al., 2020; Fernandes & Costa, 2023; Hassandoust et al., 2021). The public has significantly decreased face-to-face interactions with remote services, such as distance learning, work from home, and telecommuting (John et al., 2023; Nurse et al., 2021). The increasing demand for remote and mobile services has precipitated a growing reliance on these platforms, necessitating access to users' cameras, microphones, and sensing devices. These applications frequently ask users to give personal details for collecting, transmitting, and storing such personal information, heightening privacy concerns and reducing people's acceptance of mobile technology (Fernandes & Costa, 2023). Although these remote services and health-tracking applications contribute to epidemic management, they necessitate providing personal information and sensitive health data, eliciting individual privacy concerns (Hassandoust et al., 2021). The pandemic of 2019 has resulted in a significant increase in the use of mobile technologies among individuals, consequently

reshaping their lifestyle patterns. This trend has also amplified individual apprehensions regarding the gathering, utilizing, and distributing of personal data (Ribeiro-Navarrete et al., 2021; Wen et al., 2020).

In general, issues of mobile commerce information security and its potential misuse pose a significant threat to the confidentiality of user data (Balapour et al., 2020). Therefore, addressing these privacy issues related to mobile commerce should mitigate consumers' concerns and promote trust and acceptance of mobile commerce (Sarkar et al., 2020). Previous studies have applied the privacy calculus theory and investigated personal information disclosure behavior in mobile commerce, recognizing the mobile environment's unique privacy and security challenges (Fernandes & Costa, 2023; Hassandoust et al., 2021; Ryu, 2023; Wang et al., 2016). Thus, the present study employs the theoretical framework based on privacy calculus to explore the behaviors of user disclosure intention for accessing mobile services, mirroring the approach utilized in prior research.

Privacy calculus theory

Contemporary mobile commerce platforms require substantial volumes of personal data, which is subsequently subjected to analysis via advanced big data (Eastin & Brinson, 2017; Eastin et al., 2016) and AI algorithms (Sarker et al., 2021), thereby facilitating the delivery of convenient and intelligent personalized mobile services (Luo et al., 2023; Zhang et al., 2023). Despite apparent security and privacy concerns, researchers have discovered that consumers overlook potential privacy issues and opt to share sensitive personal data in return for intelligence and tailored mobile services (Hayes et al., 2021). In order to obtain convenient mobile services, consumers are often forced to disclose a large amount of personal information, leading to a gap between consumers' privacy concerns and actual privacy-protecting behaviors. The "privacy paradox" phenomenon has been noted within the realm of e-commerce (Kehr, Kowatsch, et al., 2015) and mobile environments (Lee & Rha, 2016; Pentina et al., 2016; Zhu et al., 2021).

Researchers have employed the "privacy calculus" concept to explore the discrepancy between individuals' stated privacy worries and their actual behavior with sensitive

technologies (Barth & de Jong, 2017). The privacy calculus refers to self-disclosure as the pros and cons of the trade-off in privacy-protective behaviors (Culnan & Armstrong, 1999; Laufer & Wolfe, 1977; Li, 2012). This theory suggests that the decision by an individual to share personal information is a subjective process viewed from an economic standpoint (Pentina et al., 2016). It indicates that privacy is not an absolute notion but rather a relative one, influenced by the individual's assessment of benefits and risks. Costs involve the risks of losing privacy, and benefits are the expected gain of individuals disclosing their private information. The theory is a rigorous framework based on the expectancy of theory and perspectives of cost-benefits (Dinev & Hart, 2006). With the expectancy of theory, an individual will act in a certain way due to what they expect from that selected behavior. According to Culnan and Bies (2003), individuals evaluate the advantages and disadvantages of sharing their private information. In other words, individuals exchange personal information to gain positive outcomes and minimize possible adverse consequences. The privacy calculus involves individuals evaluating the potential benefits and risks of sharing personal information in order to determine their comfort level with disclosure (Fox et al., 2021; Jozani et al., 2020; Liu et al., 2016; Wang et al., 2016; Zhu et al., 2021). Thus, we propose that the privacy calculus theory could describe the privacy paradox in mobile environments by balancing the potential advantages with privacy concerns before disclosing sensitive personal data for customized services (Bandara et al., 2019).

In past studies, the privacy calculus theory has been extensively adopted as a theoretical framework to examine individuals' intentions to disclose private information across various contexts, including marketing (Hayes et al., 2021), social networking services (Dienlin & Metzger, 2016; Jozani et al., 2020), e-commerce platforms (Kehr, Kowatsch, et al., 2015), and mobile environments (Fox et al., 2021; Zhu et al., 2021). With the advances in the popularity of online and mobile services, sensitive information is collected and analyzed by service providers and even exchanged between third parties without consent. Studies revealed that people's self-disclosure decisions are based on their concerns about the uncertainties and possible advantages of mobile technologies and service providers (Kehr,

Kowatsch, et al., 2015; Keith et al., 2016; Keith et al., 2013; Wang et al., 2016). Thus, the privacy calculus model is an intuitive and direct framework based on cost-benefit analysis to explain that consumers' tendency to self-disclosure decisions in online or mobile services stems from a rational evaluation of associated costs and benefits (Fernandes & Pereira, 2021; Kehr, Wentzel, et al., 2015; Plangger & Montecchi, 2020). However, it is subject to critical observation from three primary perspectives (Trepte et al., 2017). The first critique points out that individuals might be unable to fully evaluate all risks and benefits due to a lack of information, contextual constraints, and constrained cognitive capabilities (Barth & de Jong, 2017; Cho et al., 2010; Kokolakis, 2017). For instance, consumers using mobile commerce services and products may not have the ability and knowledge to identify the risks of personal data leakage that mobile commerce may bring and may have difficulty understanding information privacy concerns (Park, 2013; Park & Mo Jang, 2014; Trepte et al., 2015). This criticism implies that the theory could neglect the limitations of individuals' bounded rationality. The second critique is based on empirical research showing that when people share personal information, they are primarily driven by the expected benefits, with less emphasis on privacy concerns (Fox et al., 2021; von Kalckreuth & Feufel, 2023) and perceived risks (Kang & Namkung, 2019; Kim et al., 2019). In other words, their tendency to disclose in online shopping or use mobile services is often tied to the perceived advantages they can gain from such activities, with less emphasis on worries about potential privacy issues.

A third criticism highlights that previous studies often treat subjects uniformly, overlooking potential demographic differences and situational factors. For example, past research (Kehr, Wentzel, et al., 2015; Sun et al., 2015) has shown that demographic factors such as gender (Luo et al., 2023; Wills & Zeljkovic, 2011), age (Chakraborty et al., 2016), and cultural factors (Trepte et al., 2017), significantly impact people's concerns about information privacy. These situational factors and individual differences can influence privacy disclosure decisions beyond general attitudes and tendencies. The variability in individuals' perceptions of the benefits of privacy disclosure suggests that attitudes toward

information sharing are not uniform but influenced by personal traits related to personality rights (Sun et al., 2015). These critiques highlight a potential oversimplification in the privacy calculus theory regarding the intricate nature of individuals' privacy considerations and decision-making regarding personal information disclosure. Hence, the privacy calculus theory can be expanded by thoroughly examining individual user characteristics and investigating how situational factors influence the behaviors of sharing personal information.

Mobile privacy-related knowledge and skills

As detailed in the preceding section, the privacy calculus theory provides a rigorous framework for researchers to investigate the complex psychological aspects of personal data disclosure. The theory revealed that the rational processes account for private information disclosure behavior, meaning individuals consciously weigh risk and benefit (Barth & de Jong, 2017; Fernandes & Pereira, 2021; Kokolakis, 2017; Plangger & Montecchi, 2020). Consumers' participation in online services depends on their perception of the fairness of privacy policies and the trustworthiness of service providers (Culnan & Armstrong, 1999; Culnan & Bies, 2003; Li, 2012). Nonetheless, past studies have highlighted that one's decisions about disclosing private information can be affected by situational factors and individual disparities, apart from general attitudes and tendencies (Cho et al., 2010). This inconsistent behavior may be explained by examining the literacy of information privacy (Baruh et al., 2017). With a lack of experience with the negative consequences of private information misuse or breaches, individuals may undervalue the risks and potential harm to privacy, leading to less cautious behavior in sharing personal data (Debatin et al., 2009). In addition, individuals may lack declarative and procedural knowledge regarding privacy issues and the skills necessary to manage personal privacy information effectively. This deficiency can hinder their ability to translate privacy concerns into appropriate privacy-management actions (Debatin et al., 2009; Park, 2011; Pingo & Narayan, 2019). Therefore, a lack of privacy literacy may reduce the "fear of disclosure" and lead to higher information sharing (Epstein & Quinn, 2020).

According to protective motivation theory, simply experiencing fear or worrying about

negative consequences is not enough to help people develop self-protective behaviors; people also need to have a sense of self-efficacy (Rogers et al., 1983). That is, individuals must be able to judge vulnerability to risks and conceptualize risks as perceived vulnerability, possibility, or susceptibility (Cho et al., 2010). Therefore, when it comes to online and mobile privacy issues, users individually establish concepts and cognitive models of privacy risks, which affects how individuals process and respond to disclosing personal information (Barth et al., 2022). Several studies have found a correlation between users' awareness of information privacy concerns and their behavior. For example, awareness of data gathering risks and understanding legal protections significantly influence the relationships between concerns and behaviors (Park et al., 2012). The results show that individuals with knowledge of privacy issues and high privacy concerns exhibit the highest privacy-protective behaviors. Trepte et al. (2015) suggest that the difference between attitudes and behaviors regarding information privacy concerns may stem from a knowledge gap. Weinberger et al. (2017) also found that users' awareness of online anonymity threats was moderate, and users'general ability to take privacy and anonymity protection was low. Due to unawareness or insufficient knowledge about privacy issues and privacy protection, most online users'personal information is still accessible to others (Weinberger et al., 2017). These studies all point out that although users generally express privacy concerns, their actual behavior may not always be consistent with these concerns, which may be due to different perceptions of privacy issues. Therefore, increasing users' understanding of privacy issues can narrow the gap between expressed concerns and actual behaviors, mitigating information privacy issues (Weinberger et al., 2017). Park et al. (2012) emphasized the importance of explicit signaling within online environments, advocating for improving privacy statements customized to users' contexts. Additionally, they advocate for increasing consciousness about the security options accessible to users. Through these measures, individuals are given the means to protect their private data and strengthen their resolve to secure personal information.

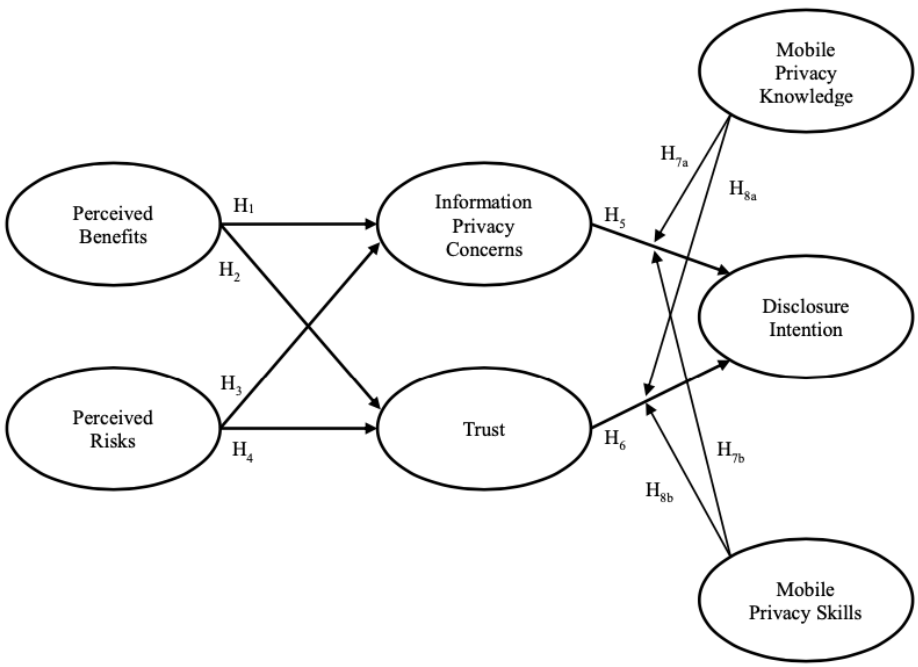
We incorporate the concept of privacy literacy to investigate drivers of the mobile commerce privacy calculus phenomenon based on mobile privacy-related knowledge

and skills (Park & Mo Jang, 2014; Weinberger et al., 2017). Past studies defined privacy literacy as the awareness and knowledge of online information practices and the ability to control personal information with strategies (Bartsch & Dienlin, 2016; Trepte et al., 2015). Debatin (2011) suggested that privacy literacy and knowledge of effective privacy protection strategies could be informed about privacy. Trepte et al. (2015) also stated that "Online privacy literacy may be defined as a combination of factual or declarative ("knowing that") and procedural ("knowing how") knowledge about online privacy." According to Trepte et al. (2015), declarative knowledge refers to the technical and legislative aspects of privacy, and procedural knowledge involves the skill of implementing privacy regulations and safeguards. Like Weinberger et al. (2017) and Prince et al. (2021), the authors also recognized that privacy knowledge and skills measure the knowledge about regulations and laws of information privacy and strategies or actions to protect personal data.

Theoretical development and hypotheses

As depicted in Figure 1., the research model proposes that (a) Information privacy concerns and trust results from a combined evaluation of perceived benefits and risks. (b) Information privacy concerns negatively affect disclosure intention; trust positively impacts disclosure intention. (c) Mobile privacy knowledge and skills moderate the link between information privacy concerns and disclosure intention. (d) Mobile privacy knowledge and skills moderate between trust and disclosure intention. The following sections discuss the rationales for these assumptions.

Figure 1
Research model



Perceived benefits and perceived risks

The perceived benefits of mobile commerce are defined as the subjective perception of advantages, usage, or adoption of mobile services. These benefits are mainly derived from (1) locationability, a result of mobile commerce's ubiquity, and (2) personalization, which is made possible by collecting and consolidating user data via mobile devices (Lee & Rha, 2016; Xu et al., 2011; Xu et al., 2009). Locationability emerges as the foundation for the widespread prevalence of mobile services, characterized by consumers' perceived ability to access requisite information or services irrespective of time and place. The concept of locationability is driven by integrating real-time geolocation tracking and map-based application programming interfaces (APIs). These technological advancements empower mobile services to offer context-sensitive information, such as suggestions for nearby retail outlets or navigation assistance, thereby setting mobile commerce apart from conventional e-commerce (Almusaylim & Jhanjhi, 2020; Ryu, 2023).

Additionally, the personalization attribute stems from mobile commerce's inherent capacity to efficiently gather and amalgamate individual preferences, thereby furnishing tailored service content. With the advances in mobile technology and mobile devices, consumers have the capability of constant connectivity and accessibility to access information and interact with one another at anytime and anywhere (Eastin et al., 2016; Wang et al., 2015). Moreover, owing to the robust data collection capabilities of mobile devices, coupled with the widespread integration of big data (Eastin & Brinson, 2017; Eastin et al., 2016) and AI algorithms (Sarker et al., 2021), users' personal information can be swiftly and comprehensively gathered, examined, and synthesized. Compared to traditional e-commerce services, the ubiquity features characteristics of mobile commerce as ease of access, personalized functionality, localization, instant connectivity, and identification (Sarkar et al., 2020; Wang et al., 2016).

The constraints associated with mobile commerce significantly curtail user acceptance and actuate privacy concerns, encompassing factors such as interface design, security of wireless connections, the potential misuse of personal data, risks associated with cellphone surveillance, and considerations of physical capability (Yeh & Li, 2009). In contrast to traditional e-commerce, mobile commerce presents distinct risks due to its dependence on data collection via integrated sensors (e.g., GPS, accelerometers) and continuous connectivity. This reliance may raise concerns regarding location tracking and unauthorized data access (Sarker et al., 2021). Mobile users are concerned that personal data could show a lack of internal controls, security breaches, and misuse by third parties without their consent, leading to distrust in mobile commerce (Wang et al., 2016). In addition, mobile devices have built-in sensors and processors that collect data, ranging from users' digital traces (e.g., GPS, online access log) to biomedical signals (e.g., heart rate, oxygen saturation) (Jozani et al., 2020). With mobile service providers' perspectives, companies and organizations can aggregate and analyze to narrowly target consumers with sensitive data, such as location, online behaviors and patterns, physiological surveillance data, and other personal data. The data are sent to mobile service providers to enhance user experience and offer personalized

services. Consumers cannot be entirely anonymous when applying mobile services due to their mobile environment traces that mobile service providers can collect, aggregate, and analyze (Eastin et al., 2016; Wessels, 2012). In order to use personalized mobile commerce services, users are required to share a large amount of personal information. Nevertheless, they may not have sufficient access to information regarding how their data is gathered and utilized, resulting in uncertainty (Al-Natour et al., 2020). This study describes perceived risk as how users perceive the risk and uncertainty associated with opportunistic behavior in mobile commerce involving personal information (Dinev & Hart, 2006).

Within mobile commerce, incorporating locationability and personalization functionalities provides users with enhanced convenience, immediacy, and tailored services. Conversely, mobile service risks underscore mobile users' concerns about the risks arising from improper collection, aggregation, and analysis of their private information, particularly in the age of extensive data accumulation and utilization facilitated by AI algorithms. The decision-making process regarding individual privacy disclosures in mobile contexts predominantly hinges on evaluating the equilibrium between perceived risks and benefits. This trade-off is consistent with the privacy calculus theory, which suggests that individuals assess the expected benefits of sharing personal information against the potential risks of privacy invasion (Dinev & Hart, 2006; Liu et al., 2016). In mobile commerce, the immediacy and context-sensitivity of services complicate this calculus, enhancing both the perceived benefits, such as instant recommendations, and the risks, like real-time tracking (Almusaylim & Jhanjhi, 2020; Lee & Rha, 2016; Ryu, 2023). This study assumes that information privacy concerns represent mobile users' concerns about the risks of improper collection and use of their private data. It also acknowledges that the perceived benefits and risks balance user worries about privacy-related issues. Therefore, the trust and concerns of users are significantly impacted by their perception of the advantages and risks associated with mobile services. The inappropriate use and over-collection of personal data can diminish users' trust in mobile commerce services and heighten worries regarding disclosing and improperly handling information privacy. Mobile services' convenience and ubiquity might strengthen

consumers' trust in operators' capabilities and alleviate privacy concerns. We propose the following research hypotheses by synthesizing the above ideas and building on the privacy calculus framework.

H1. Perceived benefits are positively related to the information privacy concerns in mobile commerce.

H2. Perceived benefits are positively related to trust in mobile commerce.

H3. Perceived risks are positively related to information privacy concerns in mobile commerce.

H4. Perceived risks are negatively related to trust in mobile commerce.

Information privacy concerns and trust

The present study defines information privacy concerns as worries about over-collection, misuse, lack of protection, and opportunistic actions associated with disclosing private information in mobile commerce contexts (Bandara et al., 2019; Bartol et al., 2023; Dinev & Hart, 2006; Li et al., 2010). From the organizational management perspective of individual data, Smith et al. (1996) described the issue of privacy concerns as organizational responsibilities in four dimensions of personal data management as perceived by users: collection, improper access, unauthorized secondary use, and error. In the online environment, Malhotra et al. (2004) indicated that organizations adopt information technology to quickly obtain, process, integrate, and transmit personal information. The information privacy concerns represent the organization's fundamental responsibility for handling customer information, but also reveal individuals' views on fairness／justice in information privacy, including collection, control, and awareness. Privacy concerns reflect how individuals perceive and internalize the potential risks of information loss (Dinev & Hart, 2006), encompassing their subjective evaluation of the appropriate use of their private data (Culnan & Armstrong, 1999; Culnan & Bies, 2003).

In previous research on mobile commerce, scholars have recognized information privacy concerns as a primary driver behind consumers' reluctance to self-disclosure (Balapour et al., 2020; Luo et al., 2023; Sarkar et al., 2020; Zhang et al., 2013). Mobile commerce intensifies

privacy concerns due to its distinct features, such as real-time geolocation tracking, map-based API interventions, and instant connectivity. These capabilities facilitate continuous data collection through built-in sensors like GPS (Lee & Rha, 2016). Consequently, users are increasingly worried about unauthorized access and the lack of transparency in data usage, as mobile devices frequently collect sensitive information, such as location and behavioral patterns, without explicit user consent (Jozani et al., 2020). The advancement of mobile technology, alongside the emergence of big data and AI algorithms, has facilitated enhanced processes for businesses and organizations to gather, consolidate, and scrutinize consumer data (Bandara et al., 2019; Eastin et al., 2016; Sarker et al., 2021). Consequently, the proliferation of mobile devices has simplified gathering substantial user data for mobile service providers and increased user concerns (Shklovski et al., 2014). Using data mining techniques and AI algorithms expedites examining and identifying consumer behavioral patterns, augmenting the company's proficiency in analyzing and targeting distinct individuals (Kang & Namkung, 2019; Khemiri & Jallouli, 2022; Khoa, 2021; Kim et al., 2019). While these advances enable businesses to identify consumer preferences, develop better mobile services, and improve customer relationships, they also increase consumers' concerns about access to and how their personal information is accessed. Mobile commerce information security issues and their potential misuse pose a significant threat to the confidentiality of user data. Therefore, in the mobile computing environment, privacy issues not only cover topics such as data collection and use but also cover broader dimensions, such as data misuse, identity theft, and lack of transparency (Sarker et al., 2021). Hence, our study delves into privacy concerns and assesses the impact on consumers' inclination to divulge personal data, encompassing data collection concerns, potential misuse, transparency, and third-party abuse (Zhang et al., 2013).

Recent scholarly inquiries have underscored the pivotal role of trust as a determinant of mobile commerce utilization, particularly given the inherent uncertainties and risks associated with mobile environments (Cho et al., 2007; Hillman & Neustaedter, 2017; Sarkar et al., 2020; Siau & Shen, 2003; Vinerean et al., 2022). Following Dinev and Hart (2006),

this study posits that trust encapsulates a confidence-based belief in mobile services' efficient, reliable, and secure processing of personal information. In mobile commerce, trust plays a critical role due to the immediacy and context-sensitivity of services, such as location-based recommendations or real-time transactions, which rely on continuous data sharing and expose users to heightened risks of data breaches or misuse (Yun et al., 2013; Zhu et al., 2017). These unique features distinguish mobile commerce from traditional e-commerce, where data collection is less pervasive and location-specific (Wang et al., 2019). Like e-commerce, trust in mobile commerce services also plays an essential role in encouraging consumers' purchase intention, continuation intention, and adoption behaviors (Hong & Cha, 2013; Khoa, 2021; Luo et al., 2023). Mobile commerce is different from traditional e-commerce in terms of user interface, inherent risks, interactivity, ubiquity, localized services and usage models (Sarkar et al., 2020; Wang et al., 2019). Therefore, when people interact with mobile technologies, users are concerned about whether the system's functions and features protect their data and privacy, such as usefulness, ease of use, system and service quality, and user interface design (Ooi et al., 2018; Sarkar et al., 2020). Multiple research studies indicate that trust in the provider plays a crucial role in shaping mobile technology acceptance and usage intentions (Lin et al., 2014; Luo et al., 2023). In other words, trust involves a person's willingness to expose themselves to the actions of another party, trusting that the other party will act in the person's best interest, regardless of supervision. Therefore, establishing user trust is crucial in interacting with users and mobile services. According to the study by Dinev and Hart (2006), we are also considering the trust beliefs from the research of McKnight et al. (2002), which encompass competence, reliability, and safety. Drawing upon the privacy calculus framework, this study formulates the following hypotheses to investigate the influence of privacy concerns and trust on the intention to disclose information in mobile commerce. This research addresses the gap in understanding the role of mobile-specific contextual factors.

H5. Information privacy concerns negatively relate to the intention to disclose information in mobile commerce.

H6. Trust positively relates to the intention to disclose information in mobile commerce.

The moderating effect of mobile privacy knowledge and skills

The privacy calculus theory assumes consumer intentions to disclose personal information are rational psychological processes (Fernandes & Pereira, 2021). The rationality perspectives of decision-making during privacy calculus assume that information disclosure behavior is an analytical and conscious approach, meaning individuals consciously weigh risks and benefits (Barth & de Jong, 2017; Kokolakis, 2017; Plangger & Montecchi, 2020). However, individuals have faced difficulties evaluating the pros and cons of self-disclosure because of their bounded rationality and limited capacity to process information (Kehr, Kowatsch, et al., 2015). These limitations include irrational thinking and thinking modes, such as intertemporal choice (Acquisti & Grossklags, 2005), desire for instant gratification and emotional responses (Anderson & Agarwal, 2011), overestimation of abilities (Princi & Krämer, 2020), and perceived level of control (Princi & Krämer, 2020). Past studies indicate that limited information, cognitive biases, heuristics, and decision-making style may be significant factors in determining the decision to share personal information (Barth & de Jong, 2017; Cho et al., 2010; Kokolakis, 2017; Meier & Krämer, 2024). These influences indicate how bounded rationality significantly shapes and influences the methodical process of carefully evaluating and considering privacy concerns.

Consumers often encounter difficulties in distinguishing between public and private domains. Therefore, users of mobile commerce services may lack the ability and awareness to recognize and understand the importance of privacy issues and potential threats (Park, 2013; Park & Mo Jang, 2014; Trepte et al., 2015), which might be explained by exploring online "privacy literacy" (Baruh et al., 2017). Cho et al. (2010) proposed that the influence of specific situational factors and individual variances on individuals' decisions regarding privacy disclosure extends beyond generalized attitudes and tendencies. Thus, individuals may lack declarative knowledge concerning privacy risks and procedural knowledge concerning safeguarding one's privacy, hindering the translation of concerns into actions for managing privacy (Debatin et al., 2009; Park, 2011; Pingo & Narayan, 2019).

The study introduces the concept of privacy literacy to investigate the critical factors

behind self-disclosure in mobile commerce, focusing on individuals' knowledge and abilities related to mobile privacy (Park & Mo Jang, 2014; Weinberger et al., 2017). Specifically, the study examines whether individuals possess declarative knowledge concerning various privacy risks and procedural knowledge regarding safeguarding privacy (Culnan & Armstrong, 1999; Kezer et al., 2016; Weinberger et al., 2017). Declarative knowledge involves understanding privacy risks, such as recognizing how mobile applications gather location data. In contrast, procedural knowledge includes the practical skills to manage privacy settings, like configuring app permissions or opting out of data tracking (Masur, 2020; Trepte et al., 2015). These two dimensions are distinct, as possessing knowledge does not always lead to effective privacy-protective behaviors, especially in the complex and ever-changing mobile commerce environment (Brough & Martin, 2020). Combining mobile privacy knowledge and skills into our research framework may help us understand the mobile commerce privacy paradox. According to Park and Mo Jang (2014), mobile privacy-related literacy can be defined as knowledge and skills regarding privacy-related activities in mobile settings. Therefore, mobile privacy knowledge is conceptualized as user awareness of personal information and location-related data institutional practices, such as knowing which mobile applications track personal data (Park & Mo Jang, 2014). The operational definition assesses individuals' static perceptions of privacy risks and data collection mechanisms, emphasizing the "knowing" level and is grounded in factual cognition (Masur, 2020; Prince et al., 2021). In addition, mobile privacy skills refer to an individual's perceptions regarding mobile data management behavior from two perspectives: personal information and location-related data (Park & Mo Jang, 2014). The operational definition focuses on evaluating dynamic skill performance, particularly assessing the user's ability to analyze and manage personal information within mobile commerce applications (Masur, 2020). It underscores the practical aspect, highlighting individuals' capacity to handle their personal privacy information effectively, for example, setting privacy permissions (Prince et al., 2021).

The research examines users' knowledge and skills related to mobile privacy, using the concept of privacy literacy to investigate the main factors that affect privacy behaviors in

mobile commerce. Past studies have revealed direct or indirect correlations between privacy literacy and concerns regarding privacy, trust, and information disclosure (Baruh et al., 2017; Weinberger et al., 2017). Individuals with privacy knowledge and skills are better equipped to manage their privacy concerns, thus strengthening the link between their willingness to share private information, trust, and acceptance of personalized services (Kang & Namkung, 2019; Rosenthal et al., 2020). For instance, individuals with procedural knowledge (mobile privacy skill) may mitigate privacy concerns by actively managing app permissions, while those with declarative knowledge (mobile privacy knowledge) may be more cautious about data-sharing practices, potentially reducing trust in services with opaque policies (Brough & Martin, 2020; Trepte et al., 2015). Privacy awareness could greatly empower these individuals to address information privacy risks and significantly shape their perceptions of privacy (Masur, 2020). In addition, individuals with privacy knowledge and skills may exhibit increased self-confidence in utilizing mobile services, which leads to disregarding privacy concerns and participating in risky behaviors (Chen & Chen, 2015; Park et al., 2012; Rosenthal et al., 2020). Past studies reveal that individuals with privacy knowledge tend to tolerate privacy concerns, have fewer privacy-related anxieties, and may be more inclined to share private information (Brough & Martin, 2020; Cho et al., 2010; Dinev & Hart, 2005). Past studies generally revealed the complex relationship between privacy concerns, knowledge, and skills (Brough & Martin, 2020). The lack of consistency in this relationship highlights the uncertainty surrounding how privacy knowledge and skills affect personal data disclosure concerns and behaviors (Prince et al., 2021).

In summary, although consumers may recognize privacy concerns and employ privacy protection measures, further research must examine how privacy knowledge and skills moderate the links between information privacy concerns, trust, and disclosure intention. Therefore, we seek to explore mobile privacy knowledge and skills moderation effect to clarify the consumer behavior inconsistency in concerns of misuse of private data, but providing private data and accepting mobile commerce services. Hence, we propose the following research hypothesis:

H7a. Mobile privacy knowledge negatively moderates the relationship between information privacy concerns and disclosure intention.

H7b. Mobile privacy skills negatively moderate the relationship between information privacy concerns and disclosure intention.

H8a. Mobile privacy knowledge positively moderates the relationship between trust and disclosure intention.

H8b. Mobile privacy skills positively moderate the relationship between trust and disclosure intention.

Method

Measurement development

We gathered data through a survey that included the specified construct items to evaluate the research model empirically. The measurement items were developed based on previous research and assessed using a 7-point Likert scale, where choices ranged from 1 (completely disagree) to 7 (completely agree). The initial item set was developed by comprehensively analyzing existing literature and theoretical considerations. After finalizing the initial questionnaire item set, a panel of scholars and practical experts in related fields reviewed each item individually for improved face validity. Following pre-testing, the questionnaire draft underwent revision and adjustment based on respondent feedback, resulting in the formal research questionnaire. All final measurement items are listed in Appendix A.

Subsequently, the following section elaborates on the questionnaire items corresponding to each construct. Perceived benefits were measured by three items, which reflect the belief that potential advantages of locationability and personalization from mobile commerce adoption, based on Dinev et al. (2013) and Zhou (2011). A five-item scale evaluated the perceived risk as the uncertainties associated with opportunistic behavior in mobile commerce involving self-disclosure derived from Malhotra et al. (2004) and Dinev & Hart (2006). Four items addressing information privacy concerns were adjusted from Dinev & Hart (2006) to represent a user's concerns about the collection, misuse, inadequate safeguarding, and opportunistic actions linked to the sensitive information shared on mobile services. In line with Dinev and Hart (2006), trust involves believing in the efficient, reliable, and secure handling of personal information in mobile services, as assessed by three items. The disclosure intention items indicate a user's readiness to share personal information in a mobile commerce platform, based on three items from Dinev and Hart (2006) and Venkatesh et al. (2003). Finally, participants' knowledge and skills in mobile privacy were evaluated through seven items, reflecting their awareness of privacy concerns and attitudes toward managing their mobile data. The original items were derived and modified from Park and

Jang (2014) for the settings of the Taiwan mobile commerce environment.

Research setting and respondents

This study mainly targets adults over 18 years old with experience using mobile commerce services. Before completing the questionnaire, participants are asked to consent to the informed consent information and review the research guidelines. The initial section of our research questionnaire focused on a demographic survey to collect background information from participants, covering age, gender, education, residency, and previous experience with mobile commerce. The following section of the questionnaire elaborates on the definition of mobile commerce services and inquires about participants' usage patterns, such as the daily duration of use and the types of devices utilized. Additionally, it assesses the specific mobile services that users have predominantly utilized. Finally, a questionnaire was administered to gather participants' attitudes concerning privacy calculus and their mobile knowledge and skills. For our research, we opted for online surveys for their suitability in addressing time, financial, and resource limitations. Our primary approach for gathering respondents was through a snowball sampling method employed within a university in Taiwan. Our participant pool consisted of students and staff members, who were incentivized to complete the questionnaire through a lottery system.

Demographic statistics of respondents

After excluding incomplete responses, we gathered data from 423 mobile commerce users, comprising students and staff from a university in Taiwan. Among them, 61.2% were female and 38.8% were male. The respondents ranged from 18 to 61 years old (Mean = 34.16, SD = 1.26), with over 70% falling between 20 and 40 years old. Most respondents held a bachelor's degree (71.4%), followed by those with graduate-level education (17.3%). The peak hours for mobile business usage were between 18:00 and 00:00, followed by 12:00 to 18:00. Primary mobile services utilized included social media, online shopping, and entertainment. Smartphones are respondents' most commonly utilized mobile devices for mobile commerce services, with tablets and wearable devices ranking next. The respondents' demographic characteristics are summarized in Table 1.

Table 1
Results of confirmatory factor analysis

Demographic Variables	Items	Frequency	%
Age	<20	95	22.5
	21-30	133	31.4
	31-40	99	23.4
	21-50	61	14.4
	51-60	27	6.4
	>61	8	1.9
Gender	Female	259	61.2
	Male	164	38.8
Education	Junior College	23	5.4
	High School	25	5.9
	Bachelor's Degree	302	71.4
	Master's Degree and Above	73	17.3
Most mobile commerce Service Usage Time*	06:00-12:00	131	
	12:00-18:00	223	
	18:00-00:00	344	
	00:00-06:00	45	
Most Usage Types of Mobile Devices*	Tablet Computer	76	
	Smartphone	409	
	Wearable Device	11	
Most Usage Types of Mobile Commerce Services*	Social Media	274	
	Shopping	313	
	Finance	95	
	Entertainment	227	
	Travel and Navigation	184	
	Health and Sport	90	
	Education	121	
	Productivity	75	
	News	160	
	Life	117	
	Others	1	

Note: * Multiple answers are allowed.

Data analysis and results

The data analysis employed structural equation modeling (SEM), which involved two main phases: measurement and structural model (Hair et al., 2021). First, the confirmatory factor analysis (CFA) was applied to test the validity and reliability of the measurement model, which demonstrates the associations between constructs and measurement items (Anderson & Gerbing, 1998; Bagozzi & Yi, 1988; Straub et al., 2004; Straub, 1989). Second, we tested the research hypothesis by constructing a structural model explaining the connections (path) between the constructs (Hair et al., 2021). We employed the IBM SPSS Amos 23.0 software package to validate the measurement and structural model. Furthermore, moderation analysis was conducted using the PROCESS Macro version 4.2 and executed in IBM SPSS 23.0 (Hayes, 2018).

Measurement model

Applying confirmatory factor analysis (CFA) aims to verify if the measurement items align with the research model constructs. The following section will elaborate on the findings of the analysis on reliability and validity. In terms of reliability, Cronbach's α, composite reliability (CR), and average variance extracted (AVE) were adapted to assess the reliability of constructs. As detailed in Table 3, Cronbach's α values for constructs ranged from .885 to .940, surpassing the commonly recommended threshold of .7 (Straub, 1989). The CR values for each construct varied between .891 and .941, exceeding the minimum acceptable threshold of .6 (Fornell & Larcker, 1981). Furthermore, the AVE for all constructs ranged from .648 to .834, surpassing the recommended value of .5 (Fornell & Larcker, 1981). Our statistical results suggest that the measurement model exhibits sufficient reliability.

Furthermore, in terms of validity, we applied and evaluated the content validity and construct validity. At the outset, the selection of measurement items is supported by existing research, leading to solid content validity. Construct validity is further evaluated through convergent and discriminant validity (Nunnally, 1994). Convergent validity is gauged by examining the item loading coefficient and the AVE. A loading coefficient greater than

.7 is considered acceptable, while loadings below .4 are eliminated (Churchill, 1979). Discriminant validity is confirmed by comparing the square root of AVE with the correlations between constructs (Fornell & Larcker, 1981). A higher square root of AVE indicates sufficient discriminant validity (Fornell & Larcker, 1981). The details of the discriminant validity test are presented in Table 4. Finally, the measurement model fit was assessed, revealing an acceptable fit: $\chi^2(441) = 1157.725$, $p < .001$, $\chi^2/df = 2.625$ (< 3; Kline, 2023), GFI = 0.840 (> 0.80; Hooper et al., 2008; Hair et al., 2019), CFI = 0.941 (> 0.90; Hu & Bentler, 1999), RMSEA = 0.062 (< 0.08), SRMR = 0.049 (< 0.05; Hu & Bentler, 1999). These results indicate that the measurement model adequately fits the data (West et al., 2021; Anderson & Gerbing, 1984).

Table 3
Factor loading, Cronbach's α, CRs, and AVEs of constructs

Constructs	Items	Loading	Cronbach's α	CR	AVE
Perceived Benefits (PB)	PB1	.872	.899	.900	.751
	PB2	.898			
	PB3	.828			
Trust (T)	T1	.877	.936	.938	.834
	T2	.939			
	T3	.923			
Perceived Risk (PR)	PR1	.826	.917	.919	.695
	PR2	.845			
	PR3	.888			
	PR4	.858			
	PR5	.743			
Information Privacy Concerns (IPC)	IPC1	.827	.940	.941	.799
	IPC2	.907			
	IPC3	.915			
	IPC4	.924			
Mobile Privacy Skills (MPS)	MPS1	.840	.925	.928	.648
	MPS2	.849			
	MPS3	.848			
	MPS4	.837			
	MPS5	.862			
	MPS6	.708			
	MPS7	.670			
Mobile Privacy Knowledge (MPK)	MPK1	.848	.936	.937	.680
	MPK2	.817			
	MPK3	.897			
	MPK4	.863			
	MPK5	.824			
	MPK6	.789			
	MPK7	.724			
Disclosure Intention (DI)	DI1	.873	.885	.891	.734
	DI2	.928			
	DI3	.760			

Note: CR (Composite Reliability), AVE (Average Variance Extracted).

Table 4
Discriminant validity: the square root of AVEs and factor correlation coefficients

Constructs	PB	T	PR	IPC	MPS	MPK	DI
PB	**.866**						
T	.358	**.913**					
PR	.422	.035	**.833**				
IPC	.504	.039	.731	**.894**			
MPS	.473	.317	.456	.488	**.805**		
MPK	.598	.110	.692	.725	.610	**.825**	
DI	.321	.612	.192	.111	.332	.302	.857

Note: The diagonal term displays the root average variance extracted (bold), while the off-diagonal term shows the correlation coefficient between the two constructs.

Structural model

The structural model analysis used SEM to evaluate the hypothesized connections among the constructs in the theoretical framework (Hair et al., 2021). Furthermore, an indirect effects analysis was undertaken by conducting a bootstrap procedure with 1,000 resamples. Figure 2 and Table 5 present the outcomes of the structural model analysis and path loadings for all proposed relationships. The perceived benefits exhibited a significant impact on both information privacy concerns ($\beta = .219$, $p < .001$) and trust ($\beta = .407$, $p < .001$), thereby supporting hypotheses 1 and 2. Furthermore, the perceived risk exerts a significant influence on information privacy concerns ($\beta = .671$, $p < .001$) and trust ($\beta = -.318$, $p < .01$), thereby providing support for hypotheses 3 and 4. The empirical analysis revealed that information privacy concerns exert a statistically non-significant influence ($\beta = .062$) on individuals' propensity to disclose information, which hypothesis 5 did not support. At the same time, trust significantly positively impacts disclosure intention ($\beta = .568$, $p<.001$), supporting hypothesis 6. Altogether, perceived benefits and risks accounted for 5.8% of the variance in information privacy concerns, wherein the perceived risks exhibited a notably

more significant influence. Furthermore, the perceived benefits and risks elucidated 13.9% of the variability in trust, with the perceived benefits manifesting a more pronounced impact. Information privacy concerns and trust accounted for 3.9% of the variance in the disclosure intention. Trust emerged as the predominant factor exerting significant influence within this context. Finally, the model fit analysis indicates that the structural equation model demonstrates good fit: $\chi^2(128) = 272.124$, $\chi^2/df = 2.126$ (< 3; Kline, 2023), GFI = 0.921 (> 0.90; West et al., 2021), CFI = 0.972 (> 0.95; Hu & Bentler, 1999), RMSEA = 0.054 (< 0.06; Hu & Bentler, 1999), SRMR = 0.048 (< 0.05; Hu & Bentler, 1999). These results suggest that the model adequately fits the data (Hair et al., 2019).

Figure 2
The structural model and moderation results

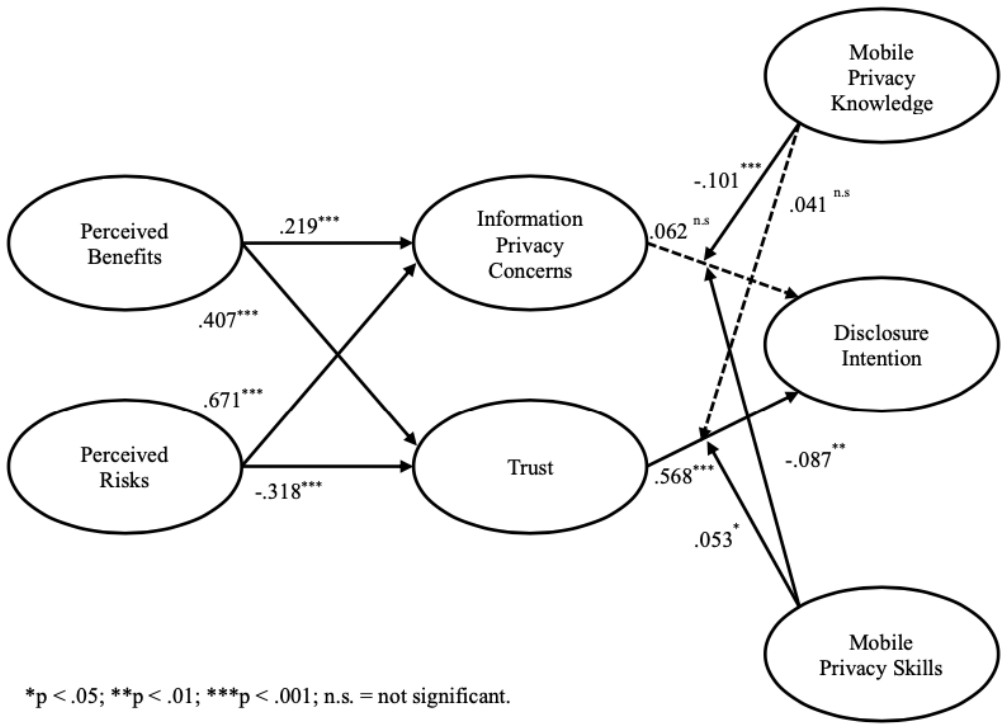


Table 5
The results of hypotheses testing

	Path	Estimate	S.E.	The results of hypotheses testing	
				Lower	Upper
H1	PB→IPC	.219***	.048	.138	.372
H2	PB→T	.407***	.067	.369	.647
H3	PR→IPC	.671***	.059	.531	.812
H4	PR→T	-.318***	.066	-.297	.013
H5	IPC→DI	.062	.051	-.309	-.032
H6	T→DI	.568***	.053	.463	.721
H7a	MPK×IPC→DI	-.101***	.030	-0160	-.042
H7b	MPS×IPC→DI	-.087**	.027	-.139	-.035
H8a	MPK×T→DI	.041 n.s.	.028	-.014	.095
H8b	MPS×T→DI	.053*	.025	.005	.101

Note: *p < .05; **p < .01; ***p < .001; n.s. = not significant.

Moderation analysis of mobile privacy knowledge and skills

Furthermore, this research examined how mobile privacy knowledge and skills moderate the relationship between factors influencing private data disclosure decision-making for mobile services. In Hypotheses 7a and 7b, we proposed that (1) an elevation in information privacy concerns is associated with a corresponding decrease in disclosure intention, and (2) this effect is enhanced by mobile privacy knowledge and skill because of the awareness of privacy issues and ability to control risk. Regarding disclosure intention and information privacy concerns, our data demonstrated that information privacy concerns have an insignificant main effect (β = .062), contrasting with prior investigations (Dienlin & Metzger, 2016; Dinev & Hart, 2006; Zhu et al., 2021). Therefore, this study sought to investigate the moderating influence within the context above.

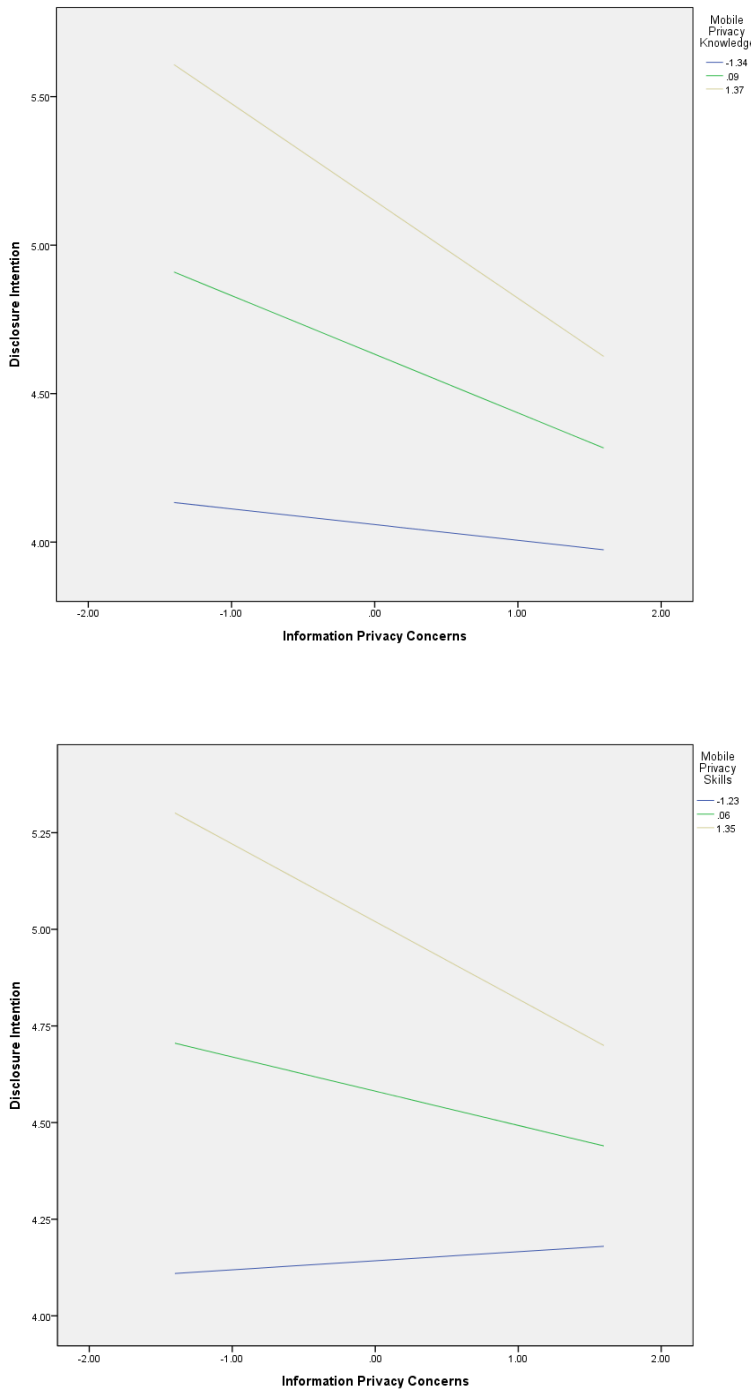
Analysis utilizing the PROCESS Macro revealed that mobile privacy knowledge exerts

a negative moderating effect on the relationship between information privacy concerns and disclosure intention (-.101, $p < .001$), and the confidence interval [-0160, -.042] did not include zero. It was determined through multiple regression analysis that the overall model was statistically significant ($F(3, 419) = 11.403$, $p = .000$, $R^2 = .117$, R^2 Changed = .024). In addition, mobile privacy skills have a negative moderation effect on the connection between information privacy concern and disclosure intention (-.087, $p < .01$), and the confidence interval [-.139, -.035] did not include zero. This data analysis result also shows that the overall model is statistically significant in the multiple regression analysis ($F(3, 419) = 18.730$, $p = .000$, $R^2 = .118$, R^2 Changed = .023). The results of the moderation analysis suggest that mobile privacy literacy exerts a moderating effect on the association between personal information privacy concerns and disclosure intentions.

The moderating effects of mobile privacy knowledge and skills on the privacy calculus are illustrated in Figure 3, wherein standardized values are stratified into three levels. According to Figure 3, we observed a negative correlation between information privacy concerns and disclosure intention. It is suggested that individuals demonstrating higher behavioral privacy literacy levels while maintaining equivalent degrees of information privacy concern exhibit an increased propensity for information disclosure. Specifically, mobile knowledge and skills exert a moderating effect, amplifying the negative relationship between information privacy concerns and disclosure intention. While privacy concerns alone did not significantly predict disclosure intention, people with elevated mobile privacy literacy (encompassing both knowledge and skills) demonstrated a reduced likelihood of information disclosure when harboring privacy concerns. This observation underscores the critical role of mobile privacy literacy in moderating the translation of privacy concerns into actual disclosure behaviors.

Figure 3

Moderation effects of Information Privacy Concerns on Disclosure Intention in (a) Mobile Privacy Knowledge and (b) Mobile Privacy Skills

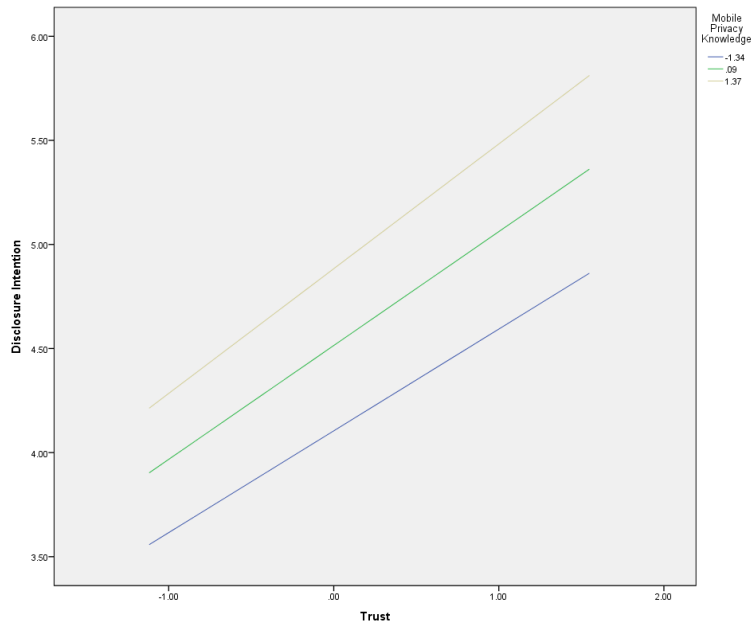


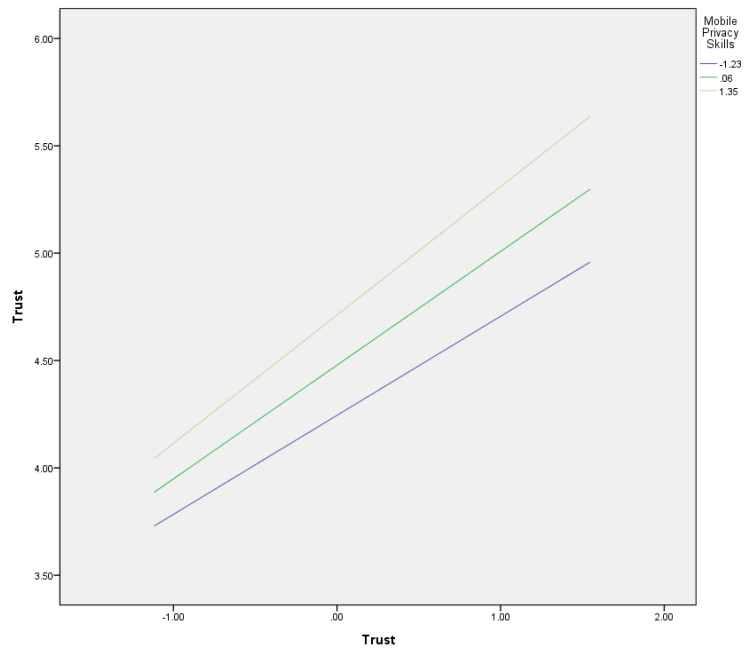
In hypotheses 8a and 8b, we postulated that (1) a heightened level of trust would positively influence disclosure intention. (2) This effect is enhanced by mobile privacy knowledge and skills, thereby augmenting user awareness of privacy concerns and risk management capabilities. Examination of the association between disclosure intention and trust revealed a substantial main effect of trust within the dataset ($\beta = .571$, $p < .001$). The non-significant moderation effect of mobile privacy knowledge in the connection between trust and disclosure intention (.041) can be seen from the results of PROCESS Macro, with the confidence interval [-.014, .095] encompassing zero. Multiple regression analysis demonstrated the statistical significance of the overarching model ($F(3, 419) = 83.349$, $p = .000$, $R^2 = .374$, R^2 Changed = .003). Conversely, the moderation effect of mobile privacy skills between information privacy concerns and disclosure exerted a positive influence (.053, $p < .05$), with the confidence interval [.005, .101] excluding zero. Multiple regression analysis similarly confirmed the statistical significance of the comprehensive model ($F(3, 419) = 74.614$, $p = .000$, $R^2 = .348$, R^2 Changed = .073). The results of our empirical analysis suggest that mobile privacy knowledge does not significantly moderate the connection between trust and disclosure intention. However, mobile privacy skills demonstrate a significant effect on this association.

Figure 4 reveals a positive correlation between trust and disclosure intention across three mobile privacy knowledge and skills levels. Our findings indicate, however, that mobile privacy knowledge and skills exhibit differential effects on the trust-disclosure intention relationship. Specifically, mobile privacy skills demonstrate a significant moderating effect, enhancing the positive association between trust and disclosure intention. In contrast, the moderating effect of mobile privacy knowledge fails to reach statistical significance. Our data analysis suggests that, within the framework of privacy calculus theory, the relationship between trust and disclosure intention is more substantially moderated by mobile privacy skills.

Figure 4

Moderation effects of Trust on Disclosure Intention in (a) Mobile Privacy Knowledge and (b) Mobile Privacy Skills





Discussion

General discussion

Based on the concept of privacy calculus, we investigate mobile service users' information privacy concerns and trust within mobile commerce from the perspectives of the perceived benefits and risks. Furthermore, it examines how information privacy concerns and trust influence mobile service users' intentions to disclose information. Most prior research implicitly or explicitly assumes that users are rational and conscious in personal information disclosure decisions while acting on privacy concerns (Barth & de Jong, 2017; Kokolakis, 2017). However, this assumption may not hold in realistic settings because users encounter external factors that may increase or decrease their rational assessment of privacy-related behavior (Barth & de Jong, 2017; Cho et al., 2010; Kokolakis, 2017). Thus, the moderation effect of mobile privacy knowledge and skills on the relations involved in the privacy calculus was also investigated. Several significant findings with theoretical and practical implications have emerged from this study.

Our research findings indicate that perceived benefits and risks correlate statistically with information privacy concerns in mobile commerce. In addition, the perceived benefits and risks also significantly shape mobile commerce trust. Consistent with previous studies (Dinev & Hart, 2006; Luo et al., 2023; von Kalckreuth & Feufel, 2023), the rapid advancements in mobile, situational awareness, and data technology empower service providers to collect, store, and aggregate consumer private information. These technologies facilitate more tailored services for consumers, concurrently amplifying apprehensions regarding privacy breaches and misuse (Almusaylim & Jhanjhi, 2020; Kang & Namkung, 2019; Xu et al., 2011). The data analysis results of the study found that people's awareness of the benefits of mobile commerce significantly increased their concerns and trust. Mobile service users will enhance trust by meeting people's needs and providing convenient and personalized services.

In contrast, people's perceived risks in mobile commerce have a statistically significant

negative impact on trust. As mentioned before, the main advantage of mobile commerce comes from providing personalized services that can be accessed ubiquitously and targeted at users (Martins et al., 2019; Zhang et al., 2023). However, mobile services have constraints, such as vulnerability to signal interception and unreliable networks, whereas personalized services facilitated by AI algorithms and big data entail inherent risks. The convenience of mobile commerce services is still inevitably overshadowed by security and privacy issues, leading to a lack of consumer trust (Khemiri & Jallouli, 2022).

Regarding factors influencing disclosure intention, the research findings indicated that information privacy concerns have no significant impact. However, previous studies have consistently shown a negative correlation between privacy concerns and self-disclosure due to apprehensions regarding privacy and security issues in information services or systems (Bansal et al., 2016; Dinev & Hart, 2006; Jozani et al., 2020). Therefore, we further clarify and explore the moderating effect of mobile privacy knowledge and skills on the negative relationship between information privacy concerns and disclosure intention. The Process Macro test results analysis reveals that mobile privacy knowledge and skills significantly moderate information privacy concerns and disclosure intention. The research results indicate that concerns about the privacy of personal information do not significantly affect disclosure intention, which might be due to the influence of situational factors related to privacy literacy. In other words, the situational factors of privacy literacy affect the intensity of information privacy concerns on disclosure intention among individuals. In addition, our research results also show that trust significantly affects mobile service users' willingness to disclose. The willingness of users to share their personal information in mobile services hinges on their trust in mobile service providers to appropriately safeguard and utilize their data. The study's findings align with previous research, indicating that trust acts as a critical link between antecedent factors (e.g., perceived benefits and risks) influencing disclosure intentions in a technological context (Dinev & Hart, 2006; Kang & Namkung, 2019; Kim et al., 2019). Our research emphasizes the essential role of trust in determining mobile service users' willingness to share personal information with operators.

This study investigated the moderating effects of mobile privacy knowledge and skills on privacy calculus in mobile commerce. The results reveal that mobile privacy knowledge and skills significantly moderate the relationship between information privacy concerns and disclosure intention. Specifically, as individuals' mobile privacy literacy increases, privacy concerns exert a more substantial negative influence on their willingness to disclose personal information, as illustrated in Figures 3a and 3b. These findings align with prior research by Masur (2020) and Kang and Namkung (2019), which suggests that higher mobile privacy literacy amplifies the negative association between privacy concerns and disclosure intention. Individuals with greater privacy knowledge and skills tend to exercise more caution in managing their personal information, reducing disclosure when privacy concerns are heightened. Conversely, those with lower privacy concerns may be more willing to share personal information in exchange for service benefits, likely due to limited awareness of privacy risks or insufficient skills to mitigate these risks. Our findings suggest that enhanced privacy literacy increases individuals' awareness of privacy risks and strengthens their ability to manage them, thereby shaping their disclosure decisions. This observation is consistent with the studies by Bartsch and Dienlin (2016) and Baruh et al. (2017), highlighting the critical role of privacy literacy in informed decision-making.

Finally, we investigated the moderating role of mobile knowledge and skills in the relationship between trust and disclosure intention. Data analysis revealed that mobile privacy skills significantly and positively moderated the effect of trust on disclosure intention (see Figure 4a). Specifically, individuals with proficient personal information management skills exhibit a reduced propensity to disclose personal data when trust in mobile services is low; conversely, they demonstrate a greater willingness to share information when trust is high. These findings indicate that individuals with advanced data management competencies strategically modulate their data-sharing behavior based on trust levels. This observation aligns with past research (Chen & Chen, 2015; Harborth & Pape, 2020; Rosenthal et al., 2020), which posited that skill-oriented competencies effectively translate trust into behavioral intentions, particularly in mobile commerce, where the practical adjustment of

privacy settings in applications is crucial. Users can manage application permissions or configure privacy settings in mobile services based on their level of trust, which means that mobile privacy skills significantly moderate the relationship between trust and disclosure intentions.

Conversely, mobile privacy knowledge does not significantly moderate the relationship between trust in mobile services and disclosure intention (see Figure 4b). This finding diverges from prior research (Rosenthal et al., 2020), which states that privacy knowledge may indirectly influence the trust-disclosure relationship by amplifying risk perceptions. As noted by Bansal et al. (2016) and Trepte et al. (2015), this discrepancy may arise because privacy knowledge increases risk awareness, but it does not necessarily translate into actionable behavior in mobile commerce settings. For example, users may be aware of privacy risks but lack the practical skills or motivation to change their disclosure behaviors, a phenomenon known as the "privacy knowledge-behavior gap" (Baruh et al., 2017; Sun et al., 2020). Furthermore, environmental factors, including sociocultural elements such as collectivist tendencies and varying expectations regarding privacy, reduce the moderating effect of knowledge within specific populations (Trepte et al., 2017). In line with previous research (Masur, 2020; Park & Mo Jang, 2014), users' disclosure behaviors appear more strongly driven by factors such as trust in the platform or reward incentives than by their knowledge of privacy. This observation may account for the lack of a statistically significant moderating effect of mobile privacy knowledge on the relationship between trust and willingness to disclose personal information. These results indicate that mobile privacy skills exert a more direct behavioral influence than knowledge in mobile commerce contexts. To further clarify the non-significant moderating role of privacy knowledge, future research could investigate the mechanisms underlying the knowledge-behavior gap, such as the role of self-efficacy in translating knowledge into action or the influence of cultural norms on privacy decision-making (Baruh et al., 2017; Trepte et al., 2017).

Research and managerial implications

The current study proposes several theoretical contributions to enhance understanding

the privacy paradox phenomenon in mobile commerce. Firstly, we extend existing research on privacy calculus by deeply exploring the privacy paradox within the mobile commerce context. By integrating mobile privacy knowledge and skills into the privacy calculus framework, we emphasize the critical role of privacy literacy in shaping personal data disclosure decisions. Specifically, mobile privacy skills significantly moderate the effects of information privacy concerns and trust on disclosure intention, enabling users to strategically adjust their data-sharing behaviors based on perceived risks or trust levels (Chen & Chen, 2015; Harborth & Pape, 2020). Conversely, mobile privacy knowledge has a more significant moderating effect on the link between information privacy concerns and the intention to disclose information, yet it does not notably influence the trust-disclosure relationship. This inconsistency may indicate a "knowledge-behavior gap," where awareness of privacy risks does not lead to actionable behaviors. This gap could be due to limited self-efficacy, complex privacy interfaces, or socio-cultural factors like collectivist norms prioritizing service benefits over privacy concerns (Baruh et al., 2017; Sun et al., 2020; Trepte et al., 2015).

Second, previous studies considering the moderation effects of mobile privacy knowledge and skills are rare (Rosenthal et al., 2020). The proposed model extends existing research by examining mobile privacy knowledge and skills as the moderation effects in the privacy calculus. This contribution is particularly significant in mobile commerce, where real-time data collection and location-based services amplify privacy concerns (Yun et al., 2013). Thirdly, our study confirms the moderating role of mobile privacy knowledge and skills in the relationships between information privacy concerns, trust, and disclosure intention, providing empirical evidence that privacy literacy offers a better explanation for the privacy paradox. The differential effects of skills (direct behavioral impact) versus knowledge (limited behavioral translation) highlight the need to incorporate nuanced literacy constructs into privacy models, thereby broadening our understanding of mobile privacy calculus from a literacy perspective (Li et al., 2017).

Drawing on our findings and existing literature, we derived several recommendations for mobile service practitioners to address user privacy concerns and foster trust. First,

mobile commerce providers could work to reduce user concerns about mobile privacy risk by redesigning privacy policies and practices, for instance, providing personalized data protection features and services based on the user's level of knowledge and ability. Mobile service providers can provide adequate privacy control features or guidelines for consumers. For instance, implementing a clear and easy understanding of privacy dashboards or guided tutorials for managing application permissions can empower users to safeguard their data effectively (Harborth & Pape, 2020).

Second, according to Barth and de Jong (2017), the mobile computing setting is a particular case; users are relatively tolerant of the risk of privacy and security intrusion in mobile applications to access mobile services or features. Although users express concerns about mobile application privacy, they may ignore them or provide personal information based on their ability to manage private information. We believe that certification or third-party verification of mobile service providers regarding regulations and systems is still crucial for building consumer confidence. Third, most app stores and providers still disclose relatively little about how to request permission for personal information in apps (Gu et al., 2017). Enhanced content and processes for mobile service providers to detail personal information management should improve consumer knowledge and alleviate privacy concerns. Practices can enhance the transparency of data consent requests by clearly explaining the purpose and benefits of collecting personal information to establish responsible data-sharing practices.

Limitations and future directions

Various limitations in the present study highlight potential directions for future research. Firstly, the main emphasis of our study is on students and faculty members from universities in Taiwan. The sample consisted primarily of university students and staff in Taiwan (n=423), collected using snowball sampling, which resulted in a relatively homogeneous distribution of age, education level, and technology usage experience. The data collection method might limit the ability to generalize the findings to the broader population of mobile commerce users in Taiwan. Future research could enhance generalizability by incorporating more diverse

populations through stratified or random sampling techniques (Meier & Krämer, 2025). Although university students and general staff are significant users of mobile services, there is an opportunity to extend future research to encompass additional demographic groups. The second limitation of this study is its primary focus on a Taiwanese sample, which constrains the generalizability of the findings to the broader Taiwanese population or other societies. Future research could broaden the sample to encompass diverse populations (Meier & Krämer, 2025). A broader range of sample diversity encompasses varied populations, which enables a more comprehensive examination of how technology access and privacy literacy interact to shape privacy behaviors in mobile commerce. For example, studies targeting the elderly (Chakraborty et al., 2016; Zeissig et al., 2017; Zou et al., 2024), low privacy literacy users (Trepte et al., 2015), or rural populations (Prince et al., 2021) could explore cognitive barriers or mobile technology infrastructure limitations to privacy disclosure decision-making in mobile commerce. Such investigations would enhance the external validity of the findings and offer insights into the contextual factors that influence privacy behaviors across diverse settings. Third, our data is only cross-sectional, and research respondents' perceptions and knowledge of mobile technology will also change over time. The cross-sectional design of this study limits the generalizability of capturing dynamic changes in privacy perceptions and behaviors. We propose that longitudinal designs or mixed-methods approaches could more effectively investigate long-term trends in privacy attitudes, such as whether the impact of mobile privacy knowledge on disclosure intentions intensifies over time. The evolution of technologies that use mobile devices to collect personal information may make it more difficult for users to perceive the severity of the invasion of personal privacy. Future mobile privacy researchers should consider the evolution of mobile technology.

As for future research directions, our study explores the role of mobile privacy knowledge and skills in moderating the privacy calculus in mobile commerce. Our findings provide insights for future research on decision-making concerning mobile commerce information disclosure and the underlying rationale and irrational and intuitive mechanisms. However, we focused exclusively on lay users' knowledge and privacy skills, excluding

those of experts (Barth et al., 2022). Therefore, it would be valuable to have future research contrast privacy experts with privacy fatigue individuals (Tang et al., 2021). Employing qualitative methodologies like scenario-based interviews, observational studies, or experimental designs could provide an understanding of privacy disclosure decision-making processes. These approaches could capture nuanced contextual factors influencing privacy behaviors by adapting various research methods. For example, longitudinal studies could reveal how privacy perceptions evolve in response to social evolution and technological advancements. These methods facilitate understanding the psychological and social factors driving information disclosure. Future research could investigate mobile privacy literacy across various contexts and frameworks, including different information and mobile systems, to clarify how privacy literacy affects variables in mobile commerce and related services.

Additionally, future studies might explore mobile privacy literacy across diverse contexts and frameworks, encompassing various information and mobile systems, to elucidate how privacy literacy influences variables in mobile commerce and related services. For instance, the rapid advancement of emerging AI technologies offers novel avenues for privacy research (Leschanowsky et al., 2024). Future investigations could examine how AI technologies reshape mobile service users' perceptions of privacy risks and privacy-related behaviors (Willems et al., 2023). Generative AI can create synthetic personal data from existing information, such as invented messages, pictures, or videos, which might heighten privacy issues and, as a result, affect decisions about sharing information (Krsek et al., 2025). The vast amount of data required for AI-driven personalization might heighten information privacy concerns regarding AI applications. Consequently, as advancements in information technology continue, it is imperative to integrate privacy concerns into contextual and technological characteristic factors. This integration will enhance our comprehension of the evolving relationship between technology and privacy-related decision-making.

Conclusions

Guided by the theory of privacy calculus, the primary objective of our study was to analyze the relationship between privacy concerns, trust, and disclosure intentions within mobile commerce. Additionally, this study explores the concept of privacy literacy in the context of mobile privacy calculus, with privacy knowledge and skills playing a role as moderation constructs in the research model. By investigating the influence of mobile commerce privacy concerns and trust on disclosure intention, this research has contributed to both theoretical understanding and practical implications. The research shows the importance of perceived benefits and risks in mobile commerce in shaping users' attitudes toward trust and information privacy concerns. Even though convenient and personalized services in mobile commerce increase trust, the risks of privacy breaches and misuse serve as significant deterrents, underscoring the delicate balance between disclosure and privacy. Moreover, contrary to conventional assumptions, this study reveals a non-significant correlation between privacy concerns and disclosure intention, indicating the complex nature of users' decision-making processes in mobile settings. The moderation effects of mobile privacy knowledge and skills shed light on the pivotal role of privacy literacy in shaping individuals' attitudes toward privacy and disclosure behavior. This study shows that mobile privacy knowledge and skills strengthen the negative relationship between information privacy concerns and self-disclosure, and mobile privacy skills heighten the positive connection between trust and disclosure intention. Hence, this study highlights the importance of understanding privacy literacy and the paradox phenomenon, which can benefit academic and practical applications in information privacy.

The results of this research are relevant for practical implications beyond the academic realm, offering actionable recommendations for mobile service providers. Strategies to alleviate users' privacy concerns, such as enhancing privacy control features and transparency in data management practices, are essential for fostering trust and promoting responsible information disclosure. Additionally, initiatives to enhance users' privacy literacy through

comprehensive guidelines and certifications can empower users to make informed decisions and mitigate privacy risks effectively. In conclusion, this study advances our understanding of privacy calculus theory in mobile commerce, emphasizing the pivotal role of perceived benefits, risks, information privacy concerns, trust, mobile privacy knowledge, and skills in shaping users' disclosure intentions. By addressing these complexities, researchers and practitioners can collaborate to navigate the evolving realm of mobile privacy and promote a safer and more transparent mobile ecosystem.

Appendix A: Research Instrument

Construct／Items	References
Perceived Benefits	
PB1: Mobile Commerce can provide 24-hours-a-day and 7-days-a-week services anytime. PB2: Mobile Commerce can provide services from anywhere (e.g., can recommend restaurants based on your current location) PB3: Mobile Commerce can provide personalized services.	Dinev et al. (2013), Zhou (2011)
Perceived Risks	
PR1: Generally, giving personal information to mobile commerce would be risky. PR2: I believe that providing personal information in mobile commerce involves the risk of losing money. PR3: I think there is uncertainty in providing personal information in mobile commerce PR4: Providing personal information in mobile commerce may encounter many unexpected problems. PR5: I feel insecure about providing personal information in mobile commerce	Malhotra et al. (2004); Dinev and Hart (2006)
Information Privacy Concerns	
IPC1: It is disturbing that mobile commerce providers ask for personal privacy information. IPC2: I am concerned about my personal information misuse by mobile commerce service providers. IPC3: I have concerns about how mobile commerce providers protect my personal information. IPC4: When using mobile commerce, personal private information may be over-collected by others.	Dinev and Hart (2006)
Trust	
T1: Mobile commerce is a safe environment to exchange information with others. T2: Mobile commerce is a reliable environment to conduct business transactions. T3: Mobile Commerce handles personal information competently submitted by users.	Dinev and Hart (2006)
Disclosure Intention	
DI1: I intend to provide personal information in mobile commerce. DI2: I intend to provide personal data in mobile commerce to obtain shopping information or services. DI3: I intend to provide my credit card number or bank account information in Mobile Commerce to make transactions or obtain personalized services.	Dinev and Hart (2006), Venkatesh et al. (2003)

Construct／Items	References
Mobile Privacy Knowledge	
MPK1: I know mobile devices and mobile commerce Apps that monitor and track personal data.	Park and Jang (2014)
MPK2: Companies or organizations can provide personalized advertising messages through information on mobile devices and mobile commerce.	
MPK3: If a mobile commerce service provider has a stated privacy policy, it does not necessarily mean they will not disclose my personal information to other companies or organizations.	
MPK4: Mobile commerce service providers may share my personal information with subsidiaries or affiliates without my consent.	
MPK5: Government privacy protection regulations do not necessarily limit the retention time for a company or organization that stored or archived private data.	
MPK6: Legal authorities can track my geographic location through mobile devices or mobile commerce Apps.	
MPK7: Mobile phone manufacturers, network operators, and service providers may have legal concerns about tracking my mobile device and mobile commerce Apps.	
Mobile Privacy Skills	
MPS1: I can carefully read the instructions for using and protecting personal information on mobile devices and mobile commerce Apps.	Park and Jang (2014)
MPS2:I can lock my mobile device and mobile commerce Apps with a password, fingerprint, or facial recognition.	
MPS3:I can modify the privacy and security settings of mobile devices and mobile commerce apps.	
MPS4:I can control the network connection settings in the mobile device, such as mobile network and Wi-Fi preferences or network sharing.	
MPS5:I can control the permission settings of mobile devices and mobile commerce apps to avoid personal information leakage.	
MPS6:I can control my mobile device and mobile commerce apps to access GPS geo-tracking data.	
MPS7: I can carefully understand which files or data inside the mobile device are used by the mobile commerce service providers.	

Acknowledgments

The author wishes to express sincere gratitude for the financial support received from Tzu Chi University of Science and Technology [Grant No. TCCT-1071A03].

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

Al-Natour, S., Cavusoglu, H., Benbasat, I., & 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), 1037-1063. https://doi.org/10.1287/isre.2020.0931

Almusaylim, Z. A., & Jhanjhi, N. Z. (2020). Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wireless Personal Communications, 111*(1), 541-564. https://doi.org/10.1007/s11277-019-06872-3

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490. https://doi.org/10.1287/isre.1100.0335

Anderson, J. C., & Gerbing, D. W. (1984). The effect of sampling error on convergence, improper solutions, and goodness-of-fit indices for maximum likelihood confirmatory factor analysis. *Psychometrika, 49*(2), 155-173. https://doi.org/10.1007/BF02294170

Anderson, J. C., & Gerbing, D. W. (1998). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423. https://doi.org/10.1037/0033-2909.103.3.411

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94. https://doi.org/10.1007/BF02723327

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International *Journal of Information Management, 52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Bandara, R., Fernando, M., & Akter, S. (2019). Privacy concerns in e-commerce: A taxonomy and a future research agenda. *Electronic Markets, 30*(3), 629-647. https://

doi.org/10.1007/s12525-019-00375-6

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21. https://doi.org/10.1016/j.im.2015.08.001

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth, S., de Jong, M. D. T., & Junger, M. (2022). Lost in privacy? Online privacy from a cybersecurity expert perspective. *Telematics and Informatics, 68*, 101782. https://doi.org/10.1016/j.tele.2022.101782

Bartol, J., Vehovar, V., & Petrovčič, A. (2023). Systematic review of survey scales measuring information privacy concerns on social network sites. *Telematics and Informatics, 85*, 102063. https://doi.org/10.1016/j.tele.2023.102063

Bartsch, M., & Dienlin, T. (2016). Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154. https://doi.org/10.1016/j.chb.2015.11.022

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

Brough, A. R., & Martin, K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology, 31*, 11-15. https://doi.org/10.1016/j.copsyc.2019.06.021

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47-56. https://doi.org/10.1016/j.dss.2015.12.007

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns

and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13-19. https://doi.org/10.1089/cyber.2014.0456

Cho, D. y., Kwon, H. J., & Lee, H. y. (2007). Analysis of trust in internet and mobile commerce adoption. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 50. https://10.1109/HICSS.2007.76

Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511*. https://doi.org/10.48550/arXiv.2003.11511

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73. https://doi.org/10.1177/002224377901600110

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342. https://doi.org/10.1111/1540-4560.00067

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 47-60). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21521-6_5

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. https://doi.org/10.1111/j.1083-

6101.2009.01494.x

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management, 50*, 261-272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior, 110*, 106382. https://doi.org/10.1016/j.chb.2020.106382

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. Sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29. https://doi.org/10.2753/JEC1086-4415100201

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295-316. https://doi.org/10.1057/ejis.2012.23

Eastin, M. S., & Brinson, N. H. (2017). Mobile commerce and the consumer information paradox: A review of practice, theory, and a research agenda. In M. Dehmer & F. Emmert-Streib (Eds.), *Frontiers in data science* (pp. 171-190). CRC Press. https://doi.org/10.1201/9781315156408-6

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior, 58*, 214-220. https://doi.org/10.1016/j.chb.2015.12.050

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society, 6*(2). https://doi.org/10.1177/2056305120916853

Fernandes, T., & Costa, M. (2023). Privacy concerns with COVID-19 tracking apps: A privacy calculus approach. *Journal of Consumer Marketing, 40*(2), 181-192. https://doi.org/10.1108/JCM-03-2021-4510

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics, 65*, 101717. https://doi.org/https://doi.org/10.1016/j.tele.2021.101717

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.1177/002224378101800104

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior, 121*, 106806. https://doi.org/10.1016/j.chb.2021.106806

Ge, Y., Liu, S., Fu, Z., Tan, J., Li, Z., Xu, S., Li, Y., Xian, Y., & Zhang, Y. (2022). A survey on trustworthy recommender systems. *arXiv preprint arXiv:2207.12515*. https://doi.org/10.48550/arXiv.2207.12515

Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19-28. https://doi.org/10.1016/j.dss.2016.10.002

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis*. Cengage Learning.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). An introduction to structural equation modeling. In J. F. Hair Jr, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, & S. Ray (Eds.), *Partial least squares structural equation modeling (PLS-SEM) using r: A workbook* (pp. 1-29). Springer International

Publishing. https://doi.org/10.1007/978-3-030-80519-7_1

Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. *SIGMIS Database, 51*(1), 51–69. https://doi.org/10.1145/3380799.3380805

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association, 28*(3), 463-471. https://doi.org/10.1093/jamia/ocaa240

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing, 55*(1), 16-30. https://doi.org/10.1016/j.intmar.2021.01.001

He, D., Chan, S., & Guizani, M. (2015). Mobile application security: Malware threats and defenses. *IEEE Wireless Communications, 22*(1), 138-144. https://doi.org/10.1109/MWC.2015.7054729

Hillman, S., & Neustaedter, C. (2017). Trust and mobile commerce in North America. *Computers in Human Behavior, 70*, 10-21. https://doi.org/10.1016/j.chb.2016.12.061

Ho, K. K. W., Chiu, D. K. W., & Sayama, K. L. C. (2023). When privacy, distrust, and misinformation cause worry about using COVID-19 contact-tracing apps. *IEEE Internet Computing, 27*(2), 7-12. https://doi.org/10.1109/MIC.2022.3225568

Hoehle, H., Scornavacca, E., & Huff, S. (2012). Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis. *Decision Support Systems, 54*(1), 122-132. https://doi.org/10.1016/j.dss.2012.04.010

Hong, I. B., & Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management, 33*(6), 927-939. https://doi.org/10.1016/j.ijinfomgt.2013.08.007

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural equation modelling: Guidelines for determining model fit. Electronic *Journal of Business Research*

Methods, 6(1), 53-60. https://doi.org/10.21427/D7CF7R

Hu, L.-t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1-55. https://doi.org/10.1080/10705519909540118

John, N., Joeckel, S., Epstein, D., & Dogruel, L. (2023). Privacy and distance learning in turbulent times: A comparison of German and Israeli schools during the beginning of the COVID-19 pandemic. *Learning, Media and Technology, 48*(3), 514-527. https://doi.org/10.1080/17439884.2022.2089682

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*, 106260. https://doi.org/10.1016/j.chb.2020.106260

Kang, J.-W., & Namkung, Y. (2019). The role of personalization on continuance intention in food service mobile apps. *International Journal of Contemporary Hospitality Management, 31*(2), 734-752. https://doi.org/10.1108/IJCHM-12-2017-0783

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635. https://doi.org/10.1111/isj.12062

Kehr, F., Wentzel, D., Kowatsch, T., & Fleisch, E. (2015). Rethinking privacy decisions: Pre-existing attitudes, pre-existing emotional states, and a situational privacy calculus. *ECIS 2015 Completed Research Papers*, 95. https://10.18151/7217379

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: Consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction (THCI), 8*(3), 88-130. https://doi.org/10.17705/1thci.00181

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

https://doi.org/10.1016/j.ijhcs.2013.08.016

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), Article 2. https://doi.org/10.5817/CP2016-1-2

Khemiri, M., & Jallouli, R. (2022). Technology-enabled personalization for mobile banking services: Literature review and theoretical framework. *Journal of Telecommunications and the Digital Economy, 10*(2), 173-194. https://doi.org/10.3316/informit.587268320552265

Khoa, B. T. (2021). The impact of the personal data disclosure's tradeoff on the trust and attitude loyalty in mobile banking services. *Journal of Promotion Management, 27*(4), 585-608. https://doi.org/10.1080/10496491.2020.1838028

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273-281. https://doi.org/10.1016/j.chb.2018.11.022

Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford Press.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Krsek, I., Kabra, A., Dou, Y., Naous, T., Dabbish, L. A., Ritter, A., Xu, W., & Das, S. (2025). Measuring, modeling, and helping people account for privacy risks in online self-disclosures with AI. *Proceedings of the ACM on Human-Computer Interaction, 9*(2), Article CSCW131. https://doi.org/10.1145/3711029

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22-42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, J.-M., & Rha, J.-Y. (2016). Personalization–privacy paradox and consumer conflict

with the use of location-based mobile commerce. *Computers in Human Behavior, 63*, 453-462. https://doi.org/10.1016/j.chb.2016.05.056

Leschanowsky, A., Rech, S., Popp, B., & Bäckström, T. (2024). Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review. *Computers in Human Behavior, 159*, 108344. https://doi.org/https://doi.org/10.1016/j.chb.2024.108344

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62-71. https://doi.org/10.1080/08874417.2010.11645450

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481. https://doi.org/10.1016/j.dss.2012.06.010

Lin, J., Wang, B., Wang, N., & Lu, Y. (2014). Understanding the evolution of consumer trust in mobile commerce: A longitudinal study. *Information Technology and Management, 15*(1), 37-49. https://doi.org/10.1007/s10799-013-0172-y

Liu, Z., Shan, J., & Pigneur, Y. (2016). The role of personalized services and control: An empirical evaluation of privacy calculus and technology acceptance model in the mobile context. *Journal of Information Privacy and Security, 12*(3), 123-144. https://doi.org/10.1080/15536548.2016.1206757

Luo, Y., Li, X., & Ye, Q. (2023). The impact of privacy calculus and trust on user information participation behavior in ai-based medical consultation-the moderating role of gender. *Journal of Electronic Commerce Research, 24*(1), 48-67.

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. https://doi.org/10.1287/isre.1040.0032

Martins, J., Costa, C., Oliveira, T., Gonçalves, R., & Branco, F. (2019). How smartphone advertising influences consumers' purchase intention. *Journal of Business Research, 94*, 378-387. https://doi.org/10.1016/j.jbusres.2017.12.047

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-

determination in the age of information. *Media and Communication, 8*(2). https://doi.org/10.17645/mac.v8i2.2855

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

Meier, Y., & Krämer, N. C. (2024). The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels. *Communication Research, 51*(2), 178-202. https://doi.org/10.1177/00936502221102101

Meier, Y., & Krämer, N. C. (2025). Differences in access to privacy information can partly explain digital inequalities in privacy literacy and self-efficacy. *Behaviour & Information Technology, 44*(6), 1183-1198. https://doi.org/10.1080/0144929X.2024.2349183

Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications, 84*, 38-54. https://doi.org/10.1016/j.jnca.2017.02.001

Nunnally, J. C. (1994). *Psychometric theory*. McGraw-Hill Education.

Nurse, J. R. C., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote working pre- and post-COVID-19: An analysis of new threats and risks to security and privacy. *HCI International 2021-Posters (Communications in Computer and Information Science)*, 1421, 583–590. https://10.1007/978-3-030-78645-8_74

Ooi, K.-B., Hew, J.-J., & Lin, B. (2018). Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach. *Behaviour & Information Technology, 37*(6), 575-595. https://doi.org/10.1080/0144929X.2018.1465997

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

Park, Y. J. (2013). Offline status, online status. *Social Science Computer Review, 31*(6), 680-702. https://doi.org/10.1177/0894439313485202

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors

of privacy protection online. *Computers in Human Behavior, 28*(3), 1019-1027. https://doi.org/10.1016/j.chb.2012.01.004

Park, Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296-303. https://doi.org/10.1016/j.chb.2014.05.041

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

Pingo, Z., & Narayan, B. (2019). Privacy literacy and the everyday use of social technologies. *Information Literacy in Everyday Life (Communications in Computer and Information Science)*, 989, 33– 49. https://10.1007/978-3-030-13472-3_4

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing, 50*(1), 32-44. https://doi.org/10.1016/j.intmar.2019.10.004

Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2021). Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management*, 1-18. https://doi.org/10.1109/TEM.2021.3092702

Princi, E., & Krämer, N. C. (2020). Out of control—privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology, 11*. https://doi.org/10.3389/fpsyg.2020.582054

Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change, 167*, 120681. https://doi.org/10.1016/j.techfore.2021.120681

Rogers, R., Cacioppo, J., & Petty, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo, R. E. Petty, & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp.

153-177). Guilford Press.

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A., & Ling, R. (2020). A tripartite model of trust in facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology, 23*(6), 840-864. https://doi.org/10.1080/15213269.2019.1648218

Ryu, S. (2023). Coupon or my privacy: How consumers choose to disclose their personal information and accept mobile location-based advertising (LBA) through privacy calculus. *Journal of Consumer Behaviour, 22*(5), 1158-1172. https://doi.org/https://doi.org/10.1002/cb.2192

Sarkar, S., Chauhan, S., & Khare, A. (2020). A meta-analysis of antecedents and consequences of trust in mobile commerce. *International Journal of Information Management, 50*, 286-301. https://doi.org/10.1016/j.ijinfomgt.2019.08.008

Sarker, I. H., Hoque, M. M., Uddin, M. K., & Alsanoosy, T. (2021). Mobile data science and intelligent apps: Concepts, AI-based modeling and research directions. *Mobile Networks and Applications, 26*(1), 285-303. https://doi.org/10.1007/s11036-020-01650-z

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management, 45*, 44-55. https://doi.org/10.1016/j.ijinfomgt.2018.10.024

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2347 – 2356. https://10.1145/2556288.2557421

Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM, 46*(4), 91–94. https://doi.org/10.1145/641205.641211

Siyal, A. W., Chen, H., Jamal Shah, S., Shahzad, F., & Bano, S. (2024). Customization at a glance: Investigating consumer experiences in mobile commerce applications.

Journal of Retailing and Consumer Services, 76, 103602. https://doi.org/10.1016/j.jretconser.2023.103602

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196. https://doi.org/10.2307/249477

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information systems, 13*(1), 24. https://doi.org/10.17705/1CAIS.01324

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169. https://doi.org/10.2307/248922

Sun, Q., Willemsen, M. C., & Knijnenburg, B. P. (2020). Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing. *Computers & Security, 97*, 101924. https://doi.org/https://doi.org/10.1016/j.cose.2020.101924

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278-292. https://doi.org/10.1016/j.chb.2015.06.006

Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management, 34*(4), 1097-1120. https://doi.org/10.1108/JEIM-03-2020-0088

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society, 3*(1), 2056305116688035. https://doi.org/10.1177/2056305116688035

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.),

Reforming european data protection law (pp. 333-365). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478. https://doi.org/10.2307/30036540

Vinerean, S., Budac, C., Baltador, L. A., & Dabija, D.-C. (2022). Assessing the effects of the COVID-19 pandemic on M-Commerce adoption: An adapted UTAUT2 approach. *Electronics, 11*(8), 1269. https://doi.org/10.3390/electronics11081269

von Kalckreuth, N., & Feufel, M. A. (2023). Extending the privacy calculus to the mHealth domain: Survey study on the intention to use mHealth apps in germany. *JMIR Human Factors, 10*, e45503. https://doi.org/10.2196/45503

Wang, S., Zhang, X., Wang, Y., & Ricci, F. (2023). Trustworthy recommender systems. *ACM Transactions on Intelligent Systems and Technology.* https://doi.org/10.1145/3627826

Wang, S. W., Ngamsiriudom, W., & Hsieh, C.-H. (2015). Trust disposition, trust antecedents, trust, and behavioral intention. *The Service Industries Journal, 35*(10), 555-572. https://doi.org/10.1080/02642069.2015.1047827

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Wang, W.-T., Ou, W.-M., & Chen, W.-Y. (2019). The impact of inertia and user satisfaction on the continuance intentions to use mobile communication applications: A mobile service quality perspective. *International Journal of Information Management, 44*, 178-193. https://doi.org/10.1016/j.ijinfomgt.2018.10.011

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science, 1*(1), 3-20. https://doi.org/10.1515/opis-2017-0002

Wen, H., Zhao, Q., Lin, Z., Xuan, D., & Shroff, N. (2020). A study of the privacy of COVID-19 contact tracing apps. *Security and Privacy in Communication Networks, Cham*, 335. https://doi.org/10.1007/978-3-030-63086-7_17

Wessels, B. (2012). Identification and the practices of identity and privacy in everyday digital communication. *New Media & Society, 14*(8), 1251-1268. https://doi.org/10.1177/1461444812450679

West, S. G., Taylor, A. B., & Wu, W. (2021). Model fit and model selection in structural equation modeling. In R. H. Hoyle (Ed.), *Handbook of structural equation modeling* (pp. 209-231). Guilford Press.

Willems, J., J., S. M., Dieter, V., Dominik, V., & and Ebinger, F. (2023). AI-driven public services and the privacy paradox: Do citizens really care about their privacy? *Public Management Review, 25*(11), 2116-2134. https://doi.org/10.1080/14719037.2022.2063934

Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management & Computer Security, 19*(1), 53-73. https://doi.org/10.1108/09685221111115863

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. https://doi.org/10.1016/j.dss.2010.11.017

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174. https://doi.org/10.2753/MIS0742-1222260305

Yeh, Y. S., & Li, Y.-M. (2009). Building trust in m-commerce: Contributions from quality and satisfaction. *Online Information Review, 33*(6), 1066-1086. https://doi.org/10.1108/14684520911011016

Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A., & Ziefle, M. (2017). Online privacy perceptions of older adults. *International Conference on Human Aspects of IT for the*

Aged Population, Cham. https://10.1007/978-3-319-58536-9_16

Zhang, F., Pan, Z., & Lu, Y. (2023). AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. I*nformation & Management, 60*(2), 103736. https://doi.org/10.1016/j.im.2022.103736

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems, 53*(4), 31-38. https://doi.org/10.1080/08874417.2013.11645648

Zhou, T. (2011). Examining mobile banking user adoption from the perspectives of trust and flow experience. *Information Technology and Management, 13*(1), 27-37. https://doi.org/10.1007/s10799-011-0111-8

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics, 61*, 101601. https://doi.org/10.1016/j.tele.2021.101601

Zou, Y., Sun, K., Afnan, T., Abu-Salma, R., Brewer, R., & Schaub, F. (2024). Cross-contextual examination of older adults' privacy concerns, behaviors, and vulnerabilities. *The 24th Privacy Enhancing Technologies (PoPETs) Symposium,* Bristol, UK, 133 - 150. https://doi.org/10.56553/popets-2024-0009