Jurnal Analisis Bisnis Ekonomi
Vol. 24 No. 1 (2026) pp. 57-75
pISSN: 1693-5950 | eISSN: 2579-647x
Journal Homepage: http://journal.unimma.ac.id/index.php/bisnisekonomi

A Multidimensional Development Theory Perspective on Mobile Fintech Privacy: Evidence from Indonesian Millennial Users

Anissa Hakim Purwantini, Betari Maharani
Department of Accounting, Faculty of Economics and Business, Universitas Muhammadiyah Magelang, Indonesia

maharani@unimma.ac.id
https://doi.org/10.31603/bisnisekonomi.v24i1.15069

Submitted: 19/10/2025 Revised: 27/03/2026 Accepted: 30/03/2026

Keywords:
Internet privacy concern;
Fintech payment;
Millenial

Abstract

Privacy has emerged as a major concern in the growing use of financial technology (FinTech) services. This study examines the factors that contribute to or mitigate Internet Privacy Concern (IPC) among Indonesian millennials who use mobile FinTech services. Drawing on Multidimensional Development Theory, the proposed research model incorporates four dimensions: environmental, individual, information management, and interaction management. Data were collected through an online questionnaire using a convenience sampling approach, yielding 432 respondents. Utilizing Structural Equation Modeling - Partial Least Squares (SEM-PLS) analysis, the results demonstrate that environmental factors play an important role in shaping internet privacy concerns among mobile FinTech payment users in Indonesia, an emerging economy. Specifically, collectivism, familiarity with government legislation, perceived benefits of information disclosure, information sensitivity, and privacy protection significantly influence internet privacy concerns. In contrast, none of the factors within the individual dimension exhibits a statistically significant effect. Similarly, industry self-regulation shows no significant influence on internet privacy concerns.

Kata kunci:
Kekhawatiran tentang privasi internet;
Pembayaran fintech;
Generasi milenial

Abstrak

Privasi menjadi kekhawatiran utama seiring dengan meningkatnya penggunaan layanan teknologi finansial (FinTech). Studi ini mengkaji faktor-faktor yang mendorong atau meredam kekhawatiran privasi di internet (Internet Privacy Concern/IPC) di kalangan generasi milenial Indonesia yang menggunakan layanan FinTech berbasis seluler. Model penelitian mendasarkan kepada Multidimensional Development Theory yang terdiri dari empat dimensi yaitu environmental, individual, information management dan interaction management. Penelitian ini menggunakan metode survei online untuk menyebarkan kuesioner kepada responden. Berdasarkan pada metode convenience sampling didapatkan 432 responden. Berdasarkan pada pengujian SEM-PLS, hasil penelitian ini membuktikan bahwa dimensi environmental menjadi peran kunci faktor yang memengaruhi internet privacy concern dalam konteks mobile FinTech Payment di negara berkembang khususnya Indonesia. Collectivism, Familiarity with government legislations, Benefit of Information Disclosure, Information Sensitivity dan Privacy Protection berpengaruh terhadap internet privacy concern. Sedangkan seluruh faktor pada individual dimension tidak berpengaruh terhadap privacy concern. Industry self-regulations juga ditemukan tidak berpengaruh signifikan.

1. Introduction

The rapid growth of financial technology (Fintech) has significantly transformed how individuals conduct financial transactions, particularly among millennials who are digital natives and extensively utilize mobile financial applications (Huang et al., 2022). Indonesia, with its substantial millennial population, has seen tremendous adoption of mobile Fintech services, driven by increasing smartphone penetration and internet accessibility. According to statistical data on peer-to-peer (P2P) lending provided by the Financial Services Authority

(OJK), as of July 2023, there were 102 registered fintech lending providers in Indonesia, comprising 95 conventional platforms and 7 sharia-based platforms. The total assets managed by these fintech lending entities amounted to IDR 7,062 billion, reflecting a significant year-on-year growth of 44.64% compared to IDR 4,882.44 billion reported in July 2022. However, alongside this growth comes heightened concerns regarding internet privacy, specifically the security of personal and financial data shared through mobile platforms (Mew & Millan, 2021).

Recent reports indicate that privacy concerns among millennials have intensified as incidences of data breaches and unauthorized use of personal information have increased (APJII, 2023). Millennials, known for their tech-savviness and active online presence, paradoxically exhibit cautious attitudes toward data sharing, shaped by their acute awareness of privacy risks in digital environments (Smith et al., 2011). Consequently, understanding the antecedents of internet privacy concerns within the context of mobile Fintech applications becomes pivotal in fostering user trust and ensuring sustainable growth in the Fintech sector.

Prior research has identified several antecedents influencing internet privacy concerns, including perceived vulnerability, perceived severity, trust, and previous privacy invasion experiences (Barth & de Jong, 2017; Hong & Thong, 2013). However, there remains limited empirical exploration specifically addressing these antecedents within mobile Fintech among millennials in emerging economies like Indonesia. Millennials' perceptions of privacy risks are distinctively nuanced by socio-cultural factors and technological familiarity, necessitating tailored investigations into their specific concerns and influencing factors (Noor, 2020).

This study extends the research model proposed by (Hong et al., 2021) by incorporating two additional factors within the environmental dimension: industry self-regulation and cultural values, particularly collectivism. These factors are especially relevant in the rapidly evolving FinTech payment industry, where regulatory frameworks and industry-led privacy protection mechanisms play an important role in safeguarding users' personal information. From a cultural perspective, individuals with stronger collectivist orientations may be more sensitive to the social consequences of financial information disclosure, particularly when unauthorized access or misuse of personal data could affect their social relationships and reputation. However, prior research has reported inconsistent findings regarding the relationship between individual-level collectivism and privacy concerns across different contexts. Against this background, examining millennial FinTech payment users in Indonesia provides an opportunity to investigate whether collectivist values are associated with heightened concerns over the collection, access, and use of personal financial and transaction data. By integrating regulatory and cultural factors, this study seeks to extend the application of Multidimensional Development Theory (MDT) to information privacy concerns in digital financial services within an emerging economy.

Therefore, this study seeks to bridge this research gap by empirically examining the antecedents of internet privacy concern within mobile Fintech contexts among Indonesian millennials. The findings aim to provide insights for policymakers and practitioners to

develop targeted privacy protection measures and enhance overall user engagement in Indonesia's dynamic Fintech landscape.

2. Literature Review

2.1. Multidimensional Development Theory

The Multidimensional Development Theory Laufer & Wolfe (1977) provides a comprehensive model comprising four dimensions that shape individuals' perceptions of privacy concerns: the individual, environmental, information management, and interaction management dimensions. The environmental dimension is defined as the boundary-setting elements that delimit the meaning and experience of privacy. Environmental factors significantly influence an individual's capacity to exercise available privacy choices; for example, differences in government regulations can affect the level of online privacy protection (Caudill & Murphy, 2000; Sarathy & Robertson, 2003). The individual dimension refers to the developmental processes through which individuals form concepts related to privacy. This dimension reflects the formation and evaluation of privacy shaped by everyday life, past experiences, and psychological factors (Hong et al., 2021; Westin, 2003). The information management dimension concerns the governance of information disclosure by balancing its benefits and risks. Finally, the interaction management dimension pertains to the management of social interactions, either among individuals or between individuals and their socio-physical environments (Hong et al., 2021).

2.2. Environmental Dimension

The environmental dimension of Internet Privacy Concern (IPC) comprises three key factors: government legislation, industry self-regulation, and cultural values. Government legislation may alleviate privacy concerns by strengthening individuals' control over their personal information. Second, industry self-regulation—rules established by firms or industry alliances—can also lower IPC, as organizational or association-level policies and procedures help safeguard consumer privacy (Culnan & Bies, 2003; Sarathy & Robertson, 2003). Third, cultural values, such as individualism and collectivism, differentially influence the level of IPC. FinTech payment services, the unauthorized disclosure of financial information or transaction histories may expose sensitive personal activities and social relationships. Consequently, millennial users with stronger collectivist values may exhibit greater concerns about the potential misuse or disclosure of such information.

H1a. Familiarity with government legislation negatively influences internet privacy concerns among millennial mobile FinTech payment users.

H1b. Industry self-regulation negatively influences internet privacy concerns among millennial mobile FinTech payment users.

H1c. Collectivism positively influences internet privacy concerns among millennial mobile FinTech payment users.

2.3. Individual Dimensions

Drawing on Multidimensional Development Theory (MDT), the individual dimension reflects how personal experiences, psychological characteristics, and knowledge

shape individuals' perceptions of privacy. Based on (Hong et al., 2021), the individual dimension comprises three factors: previous privacy invasion experience, risk avoidance, and Internet knowledge. Previous privacy invasion experience refers to a person's prior exposure to incidents involving privacy breaches. Individuals who have been victims of privacy invasion tend to exhibit higher privacy concerns due to fear arising from those adverse experiences (Dinev et al., 2013). Risk avoidance denotes a personal characteristic describing one's propensity to take or avoid risks. Individuals with higher levels of risk avoidance are more likely to develop stronger privacy concerns than those with lower levels (Hong et al., 2021). Internet knowledge pertains to individuals' perceived understanding of the Internet and its relation to privacy issues. Those with more extensive Internet knowledge are expected to form more accurate perceptions of privacy (Harris et al., 2003).

H2a. Previous privacy invasion experience positively influences Internet Privacy Concern.

H2b: Risk avoidance positively influences Internet Privacy Concern.

H2c: Internet knowledge negatively influences Internet Privacy Concern.

2.4. Information Management Dimension

Information sensitivity is defined as the degree of privacy concern elicited by the type of data requested in a particular context Information sensitivity reflects the extent to which the nature of personal data requested in a given context raises privacy concerns (Sheehan & Hoy, 2000). The more sensitive the data collected by a firm, the higher the perceived risk of misuse. Prior studies show that privacy concern increases in tandem with the sensitivity of personal information uploaded to websites (Dinev et al., 2013). Benefits of information disclosure refer to the advantages individuals obtain from sharing their information—such as monetary savings, time savings, self-enhancement, enjoyment, novelty, and altruism (Hui et al., 2006). According to (Phelps et al., 2001), privacy concern can be mitigated when firms offer meaningful benefits in exchange for personal data.

H3a. Information sensitivity positively influences Internet Privacy Concern.

H3b. Perceived benefits of information disclosure negatively influence Internet Privacy Concern.

2.5. Interaction Management Dimension

The interaction management dimension of Multidimensional Development Theory (MDT) refers to the management of social interactions between individuals and other parties or their socio-physical environment (Hong et al., 2021; Laufer & Wolfe, 1977). In the online context, this dimension emphasizes mechanisms that enable individuals to exercise greater control over information exchanges and manage privacy-related risks. Hong et al. (2021) distinguish between direct and indirect approaches to interaction management, represented by privacy protection and social presence, respectively.

Privacy protection refers to the technica and procedural safeguards adopted by websites to protect users' online privacy. To reduce individuals' privacy concerns, websites implement privacy-protection mechanisms such as obtaining user authorization before disclosing personal information (Culnan & Bies, 2003). Social presence is defined as the

extent to which a medium (e.g., a website) conveys the perceived presence of other participants in the interaction—such as the sense of a seller "being there" behind the site (Pavlou et al., 2007). A higher level of social presence fosters a sense of human connection, trust, and perceived security in online interactions, thereby reducing individuals' concerns about the privacy of their personal information.

H4a. Privacy protection negatively influences Internet Privacy Concern.

H4b. Social presence negatively influences Internet Privacy Concern.

3. Methods

3.1. Population and Sample

The population of this study comprises users of mobile FinTech products in Indonesia, specifically within the millennial generation. Based on the Financial Services Authority (OJK) report as of December 2019, approximately 70% of FinTech users in Indonesia were aged between 19 and 34 years. The sample includes consumers who have previously used mobile FinTech services, including payment platforms (e.g., OVO, GoPay, LinkAja), peer-to-peer (P2P) lending, risk management and investment platforms, or e-aggregators.

Mobile FinTech products were selected as the focus of this study because most FinTech users access services via mobile devices such as smartphones and tablets. A non-probability sampling technique was employed, specifically convenience sampling. Respondents were asked to complete an online questionnaire designed to measure their perceptions of the mobile FinTech products they have used.

3.2. Data Collection

Data were collected through an online survey (web-based questionnaire) using Google Forms, which respondents completed directly (Kennedy et al., 2011). Prior to answering the questionnaire, respondents were required to complete a screening section to determine their eligibility, which included the following questions: (1) Are you aware of mobile FinTech services? and (2) Have you ever made a transaction using a mobile FinTech service? Respondents who failed to meet these criteria were not allowed to proceed.

The questionnaire consisted of two sections: the first section captured respondents' demographic information, while the second contained closed-ended and open-ended questions designed to assess their perceptions regarding the antecedents of privacy concern in the context of mobile FinTech services.

3.3. Constructs and Sources

The variables investigated in this study consist of four dimensions of antecedents: (1) individual dimension, including previous privacy invasion experience, risk avoidance, and internet knowledge; (2) environmental dimension, including familiarity with government legislation, industry self-regulation, and cultural values (collectivism); (3) information management dimension, including information sensitivity and the perceived benefits of information disclosure; and (4) interaction management dimension, including privacy protection and social presence. This study includes 13 variables. The measurement items

were adapted from prior research, with minor modifications to suit the context of mobile FinTech. All variables were measured using a 5-point Likert scale, ranging from (1) strongly disagree to (5) strongly agree. The operational definitions and measurements for each variable are presented in **Table 1**.

Table 1. Operational of variables

Dimension	Construct	Definition	Item	Sources
Environmental	Familiarity with Government Legislation	Consumer awareness of governmental regulations concerning FinTech	2 items	(Hong et al., 2021)
	Industry self-regulation	Industry or association-established rules and procedures	3 items	(Hong et al., 2021)
	Collectivism	Consumers' collectivist cultural values	3 items	(Hong et al., 2021)
Individual	Previous privacy invasion experience	Negative experiences related to personal privacy invasion	2 items	(Malhotra et al., 2004)
	Risk avoidance	Perceptions influenced by peers, family, colleagues, supervisors, or experienced individuals considered as potential adopters	3 items	(Xu et al., 2005)
	Internet knowledge	Perceived level of consumer knowledge regarding internet use	2 items	(Singh & Hill, 2003)
Information management	Information sensitivity	Sensitivity level of data provided by consumers	2 items	(Hong et al., 2021)
	Perceived benefits of information disclosure	Perceived benefits obtained from disclosing personal information to FinTech service providers	2 items	(Hong et al., 2021)
Interaction management	Privacy protection	Privacy protection measures implemented by the FinTech industry	4 items	(Hong et al., 2021)
	Social presence	Degree of perceived interaction and communication between consumers and service providers in mobile FinTech	3 items	(Pavlou et al., 2007)
Internet privacy concern (second order construct)	Privacy concern	Concerns regarding the storage and use of personal data in mobile FinTech platforms	3 items	Hong & Thong (2013)
	Awareness	The level of individual awareness and understanding regarding what a website does with their personal data.	3 items	
	Collection	The level of individual concern regarding the amount of personal information collected by websites.	4 items	

3.4. Data Analysis and Methods

This study utilized Structural Equation Modeling - Partial Least Squares (SEM-PLS) with the aid of SmartPLS 4.0 software. SEM-PLS is suitable for complex models and small sample sizes (Abdillah & Hartono, 2015). The analysis in PLS covers both the measurement model (outer model) and the structural model (inner model).

The measurement model was assessed through validity and reliability testing. Validity tests included convergent validity and discriminant validity. Convergent validity was evaluated by factor loadings and Average Variance Extracted (AVE), with acceptable values being greater than 0.7 for loadings and above 0.5 for AVE (Hair et al., 2014). Discriminant validity was assessed by comparing the square root of AVE with the correlations between constructs. A construct exhibits discriminant validity if the square root of its AVE is higher than its correlation with any other construct, and if the cross-loadings are relatively low (Hair et al., 2019). Reliability testing was conducted to evaluate the internal consistency of measurement items. Acceptable thresholds include composite reliability and Cronbach's alpha values above 0.7, although 0.6 may be considered acceptable in exploratory research (Hair et al., 2019).

The structural model was used to evaluate the causal relationships among latent variables. The primary indicator for assessing the model fit is the R-squared (R^2) value, which reflects the proportion of variance explained by the model. Higher R^2 values indicate better explanatory power. The path coefficients in the inner model were used to test the hypotheses. Hypotheses were evaluated using the t-statistic, with a threshold of 1.64 for one-tailed tests at the 5% significance level (Hair et al., 2019).

4. Results and Discussion

4.1. Results

4.1.1. Demographic profile of the respondents

The subjects of this study were consumers who use mobile FinTech services in Indonesia, such as OVO, GoPay, LinkAja, and Dana. Data were collected over a period of two months in 2023, resulting in a total of 432 valid responses. The sample was predominantly female (65.28%) and primarily within the 20–25 years age group (82>18%). Most respondents had completed senior high school education (68.29%) and had 1 to 2 years of experience using mobile FinTech payment services (33.10%). The most frequently used FinTech services were OVO (32.41%) and GoPay (53.24%). **Table 4** shows the profil of the respondents.

4.1.2. Construct analysis

Reliability and validity tests were conducted to assess the measurement model. The results in the second test indicate that all items met the required criteria. All indicator loadings exceeded the threshold of 0.70, and the Average Variance Extracted (AVE) values for each construct were greater than 0.50, confirming convergent validity. Furthermore, the Cronbach's alpha values for all constructs were above 0.70, indicating satisfactory internal consistency. Based on these findings, it can be concluded that all variables in this study are both valid and reliable.

Table 2. Demographic profile of respondents of the study

Respondent Characteristics	Category	Number	
Gender	Male	150	34.72%
	Female	282	65.28%
Age	20–25 years	355	82.18%
	26–30 years	43	9.95%
	31–35 years	24	5.56%
	36–40 years	5	1.16%
	>40 years	5	1.16%
FinTech Usage Experience	< 6 months	143	33.10%
	6 months–1 year	93	21.53%
	1–2 years	114	26.39%
	> 2 years	82	18.98%
Education Level	Elementary School	2	0.46%
	Senior High School	295	68.29%
	Associate Degree	12	2.78%
	Bachelor's Degree	100	23.15%
	Master's Degree	23	5.32%
Monthly Income	< IDR 1,500,000	300	69.44%
	IDR 1,500,000–3,000,000	71	16.44%
	IDR 3,000,000–6,000,000	39	9.03%
	IDR 6,000,000–10,000,000	15	3.47%
	IDR 10,000,000–15,000,000	4	0.93%
	> IDR 15,000,000	3	0.69%
Monthly Usage Frequency	1–5 times	314	72.69%
	6–10 times	62	14.35%
	>10 times	56	12.96%
Preferred Mobile FinTech Service	OVO	140	32.41%
	GoPay	230	53.24%
	LinkAja	30	6.94%
	Dana	32	7.41%

Table 3. Outer loadings and collinearity statistic

Item	Outer loadings	VIF
AW <- PC	0.901	1.926
BID1 <- BID	0.942	2.060
BID2 <- BID	0.909	2.060
COLECT <- PC	0.701	1.362
FGL1 <- FGL	0.933	1.326
FGL2 <- FGL	0.774	1.326
IK1 <- IK	0.953	1.871
IK2 <- IK	0.872	1.871
INCOL1 <- COL	0.828	1.493
INCOL2 <- COL	0.871	1.690
INCOL3 <- COL	0.762	1.517
IPC <- PC	0.815	1.580
IS1 <- IS	0.755	1.242
IS2 <- IS	0.922	1.242
ISR1 <- ISR	0.962	1.172
ISR2 <- ISR	0.621	1.172
PP1 <- PP	0.845	1.978
PP2 <- PP	0.840	2.132
PP3 <- PP	0.863	2.289
PP4 <- PP	0.828	1.940
PPIE1 <- PPIE	0.787	1.293
PPIE2 <- PPIE	0.917	1.293
RA1 <- RA	0.775	1.208
RA2 <- RA	0.783	1.337
RA3 <- RA	0.750	1.417
SP1 <- SP	0.884	1.853
SP2 <- SP	0.898	1.818
SP3 <- SP	0.678	1.388

Table 4. Discriminant validity

	BID	COL	FGL	IK	IS	ISR	PP	PPIE	PC	RA	SP
BID	**0.926**										
COL	0.171	**0.822**									
FGL	0.193	0.369	**0.858**								
IK	0.419	0.142	0.267	**0.913**							
IS	0.535	0.267	0.173	0.400	**0.842**						
ISR	0.365	0.348	0.486	0.339	0.268	**0.810**					
PP	0.407	0.301	0.412	0.299	0.205	0.478	**0.844**				
PPIE	0.155	0.346	0.329	0.285	0.263	0.255	0.242	**0.855**			
PC	0.146	0.495	0.488	0.185	0.213	0.364	0.461	0.305	**0.810**		
RA	0.208	0.299	0.313	0.292	0.286	0.285	0.270	0.593	0.277	**0.770**	
SP	0.564	0.250	0.241	0.360	0.368	0.452	0.549	0.238	0.293	0.249	**0.826**

Table 5. Reliability statistic

Indicators	Composite reliability	AVE
BID	0.923	0.857
COL	0.861	0.675
FGL	0.846	0.735
IK	0.909	0.834
IS	0.829	0.710
ISR	0.784	0.655
PP	0.908	0.713
PPIE	0.843	0.730
PC	0.850	0.656
RA	0.813	0.592
SP	0.864	0.683

4.1.3. Structural Model Evaluation

Hypothesis testing was conducted using the bootstrapping method. As presented in **Table 6** and **Figure 1**, four out of ten hypotheses were supported, while the remaining six were not supported. The results indicate that familiarity with government legislation ($\beta = 0.254$, $p < 0.001$) and collectivism ($\beta = 0.293$, $p < 0.001$) have significant positive effects on internet privacy concern. However, H1a was not supported, whereas H1c was supported, as indicated in **Table 6**. Meanwhile, industry self-regulation ($\beta = 0.009$, $p = 0.433$) showed no statistically significant effect on internet privacy concern, indicating that H1b was not supported.

Table 6. Hypothesis testing

	Original sample	T statistics	P values	Result
FGL → PC	0.254	4.498	0.000	H1a (-): Not supported
ISR → PC	0.009	0.170	0.433	H1b (-): Not supported
COL → PC	0.293	4.504	0.000	H1c (+): Supported
PPIE → PC	0.040	0.910	0.181	H2a (+): Not supported
RA → PC	0.008	0.151	0.440	H2b (+): Not supported
IK → PC	-0.013	0.311	0.378	H2c (-): Not supported
IS → PC	0.083	1.658	0.049	H3a (+): Supported
BID → PC	-0.140	2.585	0.005	H3b (-): Supported
PP → PC	0.269	5.106	0.000	H4a (-): Not supported
SP → PC	0.049	0.995	0.160	H4b (-): Not supported

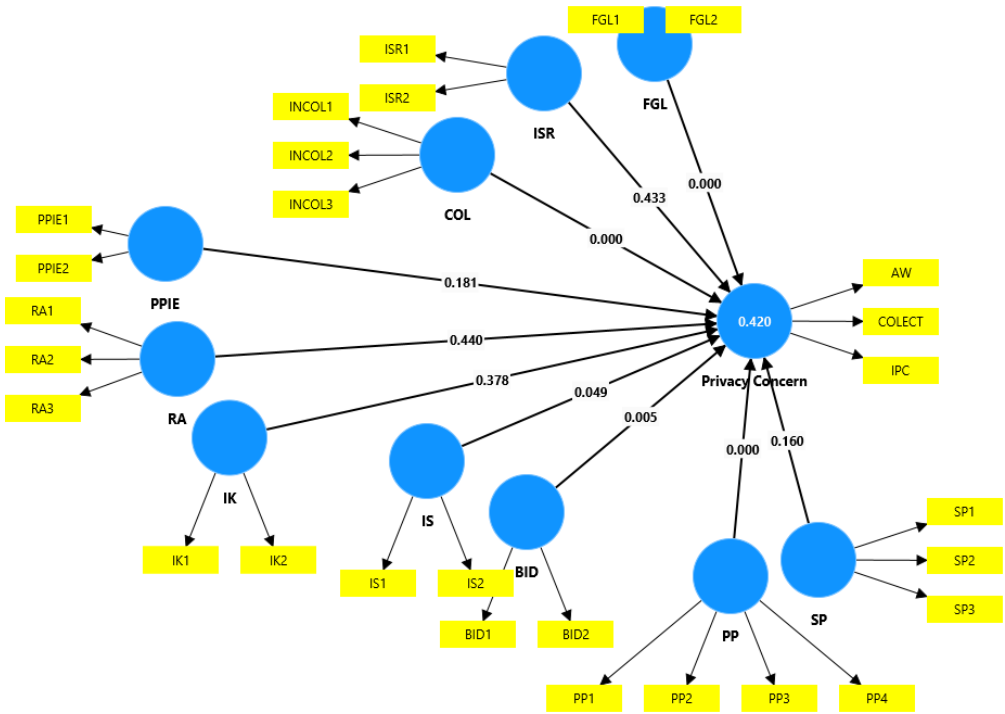


Figure 1. Structural model evaluation

Furthermore, previous privacy invasion experience (β = 0.040, p = 0.181), risk avoidance (β = 0.008, p = 0.440), and internet knowledge (β = −0.013, p = 0.378) did not exhibit statistically significant effects on internet privacy concern. Thus, H2a, H2b, and H2c were not supported. In contrast, information sensitivity (β = 0.083, p = 0.049) and perceived benefits of information disclosure (β = −0.140, p = 0.005) demonstrated statistically significant effects on internet privacy concern, supporting H3a and H3b, respectively. Notably, perceived benefits of information disclosure exhibited a significant negative relationship with internet privacy concern. Privacy protection (β = 0.269, p < 0.001) had a significant positive effect on internet privacy concern, so H4a was not supported. Meanwhile, social presence (β = 0.049, p = 0.160) did not significantly affect internet privacy concern, indicating that H4b was not supported.

4.2. Discussion

This study adopts the Multidimensional Development Theory (MDT) to examine the antecedents of Internet Privacy Concern (IPC) among millennial consumers in the context of mobile FinTech payment services. Several noteworthy findings have emerged from the analysis.

4.2.1. Environmental Dimension

The findings reveal that environmental factors play a differentiated role in shaping Internet Privacy Concern (IPC) among millennial mobile FinTech payment users in Indonesia. Specifically, familiarity with government legislation (H1a) and collectivism (H1c) exhibit significant relationships with IPC, whereas industry self-regulation (H1b) does not.

These findings highlight the distinct roles of regulatory awareness, industry-led safeguards, and cultural values in shaping individuals' privacy perceptions.

First, familiarity with government legislation has a significant positive relationship with Internet Privacy Concern (IPC), contrary to the hypothesized negative relationship and previous findings (Hong et al., 2021). This result is consistent with prior evidence suggesting that greater privacy literacy and knowledge of data protection regulations do not necessarily reduce privacy concerns (Prince et al., 2023). In the Indonesian context, this relationship may reflect a gap between regulatory awareness and confidence in legal enforcement. Although Law No. 27 of 2022 on Personal Data Protection and Bank Indonesia Regulation No. 23/6/PBI/2021 establish legal safeguards for personal and payment-related information, challenges in implementing the personal data protection framework and establishing a dedicated supervisory authority may undermine perceived regulatory effectiveness. Consequently, users who are more familiar with privacy legislation may also be more aware of potential data misuse and limitations in enforcement, leading to heightened concerns about the security of their personal and financial information in mobile FinTech payment services.

Second, industry self-regulation does not exhibit a statistically significant relationship with IPC, providing no support for H1b. This finding suggests that industry-led privacy mechanisms may not necessarily alleviate users' privacy concerns. Privacyh general structural assurance differs conceptually from industry self-regulation, their findings suggest that broad institutional assurances may be insufficient to alleviate privacy concerns. Culnan & Bies (2003) highlighted the limitations of industry self-regulation, demonstrating that the presence of privacy disclosures does not necessarily indicate comprehensive privacy protection. In the Indonesian FinTech payment context, the nonsignificant relationship may reflect limited user awareness of industry-led privacy standards or uncertainty regarding their effectiveness and enforcement. However, these explanations require further investigation. Importantly, the findings do not imply that industry self-regulation is ineffective in protecting personal data; rather, its hypothesized direct relationship with users' privacy concerns was not empirically supported. This distinction suggests that the existence of industry-led safeguards and users' perceptions of their effectiveness should be considered separately.

Third, collectivism has a significant positive relationship with Internet Privacy Concern (IPC), supporting H1c. This finding is consistent with Abbas & Mesch (2015) who demonstrated a positive association between individual-level collectivism and privacy concerns among Facebook users. Similarly, Kao & Sapp (2022) found that collectivist values heightened privacy concerns in the context of government network surveillance. These findings suggest that collectivism does not necessarily reduce individuals' sensitivity to privacy threats but may increase their concerns about the potential social consequences of unauthorized information disclosure. Abbas & Mesch (2015) further explained that collectivist individuals tend to distinguish between in-group and out-group members, making them particularly concerned about losing control over the disclosure of personal information beyond their trusted social circles. Supporting this interpretation, Fleming et al. (2021) highlighted the sensitivity of group-oriented individuals to potential harms arising from

unintended information disclosure. In the context of mobile FinTech payment services, unauthorized access to financial information and transaction histories may expose sensitive personal activities and social relationships. Consequently, millennial users with stronger collectivist orientations may exhibit greater privacy concerns because of the potential social and reputational consequences of financial data misuse. This finding extends the application of Multidimensional Development Theory (MDT) by highlighting the relevance of individual-level cultural values in shaping privacy concerns within digital financial services in an emerging economy.

4.2.2. Individual Dimensions

The findings reveal that none of the three individual factors, i.e. previous privacy invasion experience, risk avoidance, and Internet knowledge, has a statistically significant relationship with Internet Privacy Concern (IPC), providing no support for H2a, H2b, and H2c. These results contrast with Hong et al. (2021), who found significant relationships between all three individual factors and IPC. This divergence suggests that the relevance of individual antecedents may vary across digital service contexts, particularly when privacy concerns involve sensitive financial information and established payment platforms.

First, previous privacy invasion experience does not significantly influence IPC, providing no support for H2a. This finding is consistent with Zhao et al. (2012), who found that previous privacy invasions did not significantly affect privacy concerns among users of location-based social networking services. Although negative privacy experiences are generally expected to increase concerns about future violations, their influence may depend on the relevance of those experiences to the current service context. Martin & Shilton (2016) demonstrated that mobile application users' privacy judgments are shaped by the interaction between individual preferences, contextual factors, and prior experience with applications. In the mobile FinTech payment context, users may evaluate privacy risks primarily in relation to current data-handling practices and available safeguards rather than relying solely on previous privacy violations. Thus, the nonsignificant relationship suggests that prior privacy invasion experience is not necessarily a direct determinant of IPC across different digital service environments.

Second, risk avoidance does not exhibit a statistically significant relationship with IPC, providing no support for H2b. This result differs from Hong et al. (2019), who identified risk avoidance as a significant positive predictor of privacy concerns. Nevertheless, the present finding may be interpreted through the context-dependent nature of privacy judgments. Martin & Shilton (2016) demonstrated that general privacy preferences have limited explanatory power for privacy judgments in specific mobile application scenarios, highlighting the importance of contextual factors and information-use practices. Similarly, Barth & de Jong (2017) emphasized that online privacy decisions involve contextual evaluations of risks and benefits rather than relying exclusively on general individual dispositions. In mobile FinTech payment services, users may distinguish their general tendency to avoid risks from concerns about how service providers collect, manage, and protect financial information. Accordingly, the findings suggest that general risk-avoidance

tendencies may be insufficient to explain IPC when service-specific privacy considerations are considered. However, this interpretation warrants further empirical investigation.

Third, Internet knowledge does not significantly influence IPC, providing no support for H2c. This finding is consistent with Ma & Chen (2023) who reported a nonsignificant relationship between subjective privacy literacy and privacy concerns among Chinese digital natives. Their study further demonstrated that subjective and objective privacy literacy have different relationships with privacy concerns, indicating that perceived knowledge does not necessarily correspond to actual privacy-related competence. Hong et al. (2021) also acknowledged inconsistencies in earlier findings regarding the relationship between Internet knowledge and privacy concerns. Greater Internet knowledge may simultaneously enhance individuals' ability to protect personal information and increase their awareness of potential privacy threats, potentially producing competing effects. In the mobile FinTech payment context, general Internet knowledge may therefore be insufficient to reduce concerns about complex financial data practices, including transaction monitoring, data sharing, and unauthorized information use. The findings highlight the importance of distinguishing general Internet knowledge from privacy-specific knowledge and users' understanding of financial data protection mechanisms.

Taken together, these findings provide a context-specific perspective on the individual dimension of MDT. Contrary to Hong et al. (2021), none of the individual antecedents examined in this study significantly explains IPC among millennial mobile FinTech payment users in Indonesia. These results suggest that personal experiences, risk dispositions, and Internet knowledge do not necessarily translate into stronger or weaker privacy concerns across digital service contexts. Rather, privacy concerns may be more closely associated with the characteristics of information disclosure and the privacy safeguards provided by digital financial service providers. By demonstrating the limited direct explanatory role of the individual factors in this context, the present study extends the empirical application of MDT and highlights the importance of examining privacy determinants within specific digital service environments.

4.2.3. Information Management Dimension

The findings reveal that both information sensitivity and perceived benefits of information disclosure significantly influence Internet Privacy Concern (IPC), supporting H3a and H3b. These results are consistent with Hong et al. (2021), who demonstrated that information sensitivity increases IPC, whereas the perceived benefits of information disclosure reduce it. From the perspective of Multidimensional Development Theory (MDT), these findings reinforce the relevance of information management in shaping privacy concerns, particularly through the risk–benefit considerations underlying the privacy calculus framework (Dinev et al., 2013).

First, information sensitivity has a significant positive relationship with IPC, supporting H3a. This finding aligns with Hong et al. (2021) and Jozani et al. (2020) who found that perceived information sensitivity increases privacy concerns. Phelps et al. (2001) similarly demonstrated that consumers' privacy concerns vary depending on the type of

personal information requested. In the context of mobile FinTech payments, users are required to disclose sensitive information, including personal identification details, financial information, and transaction-related data. The perceived sensitivity of such information may heighten concerns about unauthorized access, secondary use, and potential financial or reputational consequences. Thus, the findings suggest that the sensitivity of information requested by FinTech providers remains an important consideration in users' privacy evaluations, even when information disclosure is necessary to access payment services.

Second, perceived benefits of information disclosure have a significant negative relationship with IPC, supporting H3b. This finding is consistent with Hong et al. (2019), who demonstrated that perceived disclosure benefits alleviate privacy concerns. It is also consistent with the broader privacy calculus perspective, which suggests that individuals consider the benefits and potential risks associated with disclosing personal information (Dinev et al., 2013). In the mobile payment context, Yang et al. (2020) found that perceived benefits contribute to users' evaluations of information disclosure, while Shalihah et al. (2023) demonstrated that perceived benefits positively influence disclosure intentions among Indonesian e-wallet users. Although these studies examined disclosure-related outcomes rather than IPC directly, they reinforce the relevance of perceived benefits in digital payment environments. For millennial FinTech payment users, benefits such as transaction convenience, time efficiency, and service accessibility may increase the perceived value of providing personal information, thereby alleviating privacy concerns. These findings suggest that users' privacy evaluations are shaped not only by potential information-related risks but also by the benefits obtained through disclosure.

4.2.4. Interaction Management Dimension

The findings reveal that privacy protection significantly reduces Internet Privacy Concern (IPC), supporting H4a, whereas social presence does not exhibit a statistically significant relationship with IPC, providing no support for H4b. These results partially align with Hong et al. (2019), who found that both privacy protection and social presence negatively influenced IPC. From the perspective of Multidimensional Development Theory (MDT), these findings suggest that direct privacy protection mechanisms and indirect social interaction mechanisms may differ in their relevance to privacy concerns within mobile FinTech payment services.

Privacy protection has a significant positive relationship with Internet Privacy Concern (IPC), contrary to the hypothesized negative relationship. This unexpected finding may reflect heightened privacy awareness and risk salience, whereby privacy protection mechanisms, such as consent requests, privacy notices, and data access controls, make users more conscious of potential threats to their personal information. Previous research suggests that privacy concerns are positively associated with the adoption of privacy-protective measures (Baruh et al., 2017), while greater transparency does not necessarily alleviate privacy-related reservations (Karwatzki et al., 2017). In the Indonesian FinTech payment context, this relationship may also reflect users' uncertainty regarding the effectiveness of data protection practices, particularly given the challenges associated with safeguarding

personal and financial information (Rohendi & Kharisma, 2024). Thus, stronger perceptions of privacy protection may coexist with heightened privacy concerns, suggesting that the availability of protective mechanisms alone may be insufficient to reassure users without demonstrable effectiveness and trustworthiness.

Second, social presence does not significantly influence IPC, providing no support for H4b. This finding contrasts with Hong et al. (2021), who identified social presence as a significant factor in reducing privacy concerns. However, Tu (2002) reported a nonsignificant correlation between social presence and online privacy in computer-mediated communication environments, suggesting that perceived interpersonal presence does not necessarily correspond to stronger perceptions of privacy. Furthermore, Kaushik et al., (2018) found a positive relationship between social presence and website-specific privacy concerns, indicating that its influence may vary across digital contexts. In mobile FinTech payment services, interactions are primarily transaction-oriented and often conducted through automated interfaces with limited interpersonal engagement. Consequently, users may place greater emphasis on the security and confidentiality of their financial information than on the perceived presence of other individuals during digital interactions. Although social presence may enhance interpersonal connection and perceived service accessibility, these characteristics may not necessarily alleviate concerns about unauthorized data access, disclosure, or misuse.

5. Conclusion

This study extends the application of Multidimensional Development Theory (MDT) by examining the determinants of internet privacy concerns (IPC) among millennial mobile FinTech payment users in Indonesia. The findings reveal that environmental, information management, and interaction management factors play significant roles in shaping IPC. Specifically, collectivism, familiarity with government legislation, perceived benefits of information disclosure, information sensitivity, and privacy protection exhibit significant relationships with IPC. In contrast, none of the individual factors shows a statistically significant relationship, while industry self-regulation is also found to be insignificant. These findings extend the empirical understanding of MDT by demonstrating that the relevance of privacy determinants varies across dimensions and contexts. In particular, the significant role of collectivism highlights the importance of incorporating cultural values into privacy research, while the insignificant individual factors suggest that established privacy determinants may operate differently in digital financial services within emerging economies.

From a practical perspective, these findings offer important implications for FinTech payment providers, industry associations, and policymakers. FinTech providers should strengthen privacy protection mechanisms, enhance transparency regarding the collection and use of personal information, and clearly communicate the benefits and potential risks associated with information disclosure. Given the significant role of collectivism, privacy management strategies should also consider users' sensitivity to the potential social and reputational consequences of unauthorized financial data disclosure. Furthermore,

policymakers should improve public understanding of personal data protection regulations to support informed privacy decisions. Although industry self-regulation does not exhibit a significant relationship with IPC, this finding highlights the need to further examine the visibility, credibility, and perceived effectiveness of industry-led privacy safeguards rather than assuming that their mere existence is sufficient to alleviate users' concerns.

Despite its contributions, this study has several limitations. First, its focus on millennial FinTech payment users in Indonesia may limit the generalizability of the findings to other generations, countries, and digital financial services. Future research could conduct cross-generational and cross-cultural comparisons to examine whether the identified relationships remain consistent across different demographic and institutional contexts. Second, as this study primarily examines the antecedents of Internet Privacy Concern (IPC), future research could extend the model by incorporating behavioral outcomes within the Antecedents–Privacy Concerns–Outcomes (APCO) framework (Smith et al., 2011). Specifically, integrating the multidimensional antecedents of IPC with continuance intention to use mobile FinTech payment services would provide a more comprehensive understanding of how privacy concerns relate to users' sustained engagement with digital financial services. Finally, longitudinal studies incorporating actual usage behavior could offer further insights into how privacy concerns and continuance decisions evolve alongside technological advancements and changes in the regulatory environment.

Authors' Declaration

Authors' contributions and responsibilities

The authors made substantial contributions to the conception and design of the study. The authors took responsibility for data analysis, interpretation and discussion of results. The authors read and approved the final manuscript.

Funding

This research is partly funded by the Universitas Muhammadiyah Magelang, Indonesia.

Availability of data and materials

All data are available from the authors.

Competing interests

The authors declare no competing interest.

Additional information

No additional information from the authors.

References

Abbas, R., & Mesch, G. S. (2015). Cultural values and Facebook use among Palestinian youth in Israel. *Computers in Human Behavior*, *48*, 644–653. https://doi.org/10.1016/j.chb.2015.02.031

Abdillah, W., & Hartono, J. (2015). *Partial Least Square (PLS): Alternatif Structural Equation Modeling (SEM) dalam Penelitian Bisnis*. Andi.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2023). *Survei penetrasi & perilaku*

internet 2023.

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

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

Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing*, *19*(1), 7–19. https://doi.org/10.1509/jppm.19.1.7.16951

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

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

Fleming, P., Bayliss, A. P., Gareth Edwards, S., & Seger, C. R. (2021). The role of personal data value, culture and self-construal in online privacy behaviour. *PLoS ONE*, *16*(7 July), e0253568. https://doi.org/10.1371/journal.pone.0253568

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Harris, M. M., Van Hoye, G., & Lievens, F. (2003). Privacy and attitudes towards Internet-based selection systems: A cross-cultural comparison. *International Journal of Selection and Assessment*, *11*(2–3), 230–236. https://doi.org/10.1111/1468-2389.00246

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics*, *168*(3), 539–564. https://doi.org/10.1007/s10551-019-04237-1

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly: Management Information Systems*, *37*(1), 275–298. https://doi.org/10.25300/MISQ/2013/37.1.12

Huang, X., Chau, K. Y., Tang, Y. M., & Iqbal, W. (2022). Business Ethics and Irrationality in SME During COVID-19: Does It Impact on Sustainable Business Resilience? *Frontiers in Environmental Science*, *10*, 1–13. https://doi.org/10.3389/fenvs.2022.870476

Hui, K. L., Tan, B. C. Y., & Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology*, *6*(4), 415–441. https://doi.org/10.1145/1183463.1183467

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

Kao, Y. H., & Sapp, S. G. (2022). The effect of cultural values and institutional trust on public perceptions of government use of network surveillance. *Technology in Society*, *70*, 102047. https://doi.org/10.1016/j.techsoc.2022.102047

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, *34*(2), 369–400. https://doi.org/10.1080/07421222.2017.1334467

Kaushik, K., Kumar Jain, N., & Kumar Singh, A. (2018). Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications*, *32*, 57–68. https://doi.org/10.1016/j.elerap.2018.11.003

Kennedy, H. P., Farrell, T., Paden, R., Hill, M. S., Rima Jolivet, R., Cooper, B. A., & Rising, S. S. (2011). A randomized clinical trial of group prenatal care in two military settings. *Military Medicine*, *176*(10), 1169–1177. https://doi.org/10.7205/MILMED-D-10-00394

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

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

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

Martin, K., & Shilton, K. (2016). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, *67*(8), 1871–1882. https://doi.org/10.1002/asi.23500

Mew, J., & Millan, E. (2021). Mobile wallets : key drivers and deterrents of consumers ' intention to adopt ABSTRACT. *The International Review of Retail, Distribution and Consumer Research*, *31*(2), 182–210. https://doi.org/10.1080/09593969.2021.1879208

Noor, M. U. (2020). Indonesian millennial awareness to privacy and personal data protection on the internet. *DESIDOC Journal of Library and Information Technology*, *40*(2), 431–436. https://doi.org/10.14429/djlit.40.02.14969

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 105–136.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, *15*(4), 2–17. https://doi.org/10.1002/dir.1019

Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2023). 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*, *70*(10), 3553–3570. https://doi.org/10.1109/TEM.2021.3092702

Rohendi, A., & Kharisma, D. B. (2024). Personal data protection in fintech: A case study from Indonesia. *Journal of Infrastructure Policy and Development*, *8*(7), 4158. https://doi.org/10.24294/jipd.v8i7.4158

Sarathy, R., & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics*, *46*(2), 111–126. https://doi.org/10.1023/A:1025001627419

Shalihah, A. H., Ruldeviyani, Y., Saraswati, K., & Ar Rasyiid, A. (2023). An Empirical Investigation of Factors Affecting Personal Information's Disclosure on Mobile Payment (E-Wallet) Platforms. *International Journal on Advanced Science, Engineering and Information Technology*, *13*(3), 1031–1040. https://doi.org/10.18517/ijaseit.13.3.18054

Singh, T., & Hill, M. E. (2003). Consumer privacy and the Internet in Europe: a view from Germany. *Journal of Consumer Marketing*, *20*(7), 634–651.

https://doi.org/10.1108/07363760310506175

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly: Management Information Systems*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Tu, C.-H. (2002). The relationship between social presence and online privacy. *The Internet and Higher Education*, *5*(4), 293–318. https://doi.org/10.1016/S1096-7516(02)00134-3

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Xu, H., Teo, H. H., & Tan, B. C. Y. (2005). Predicting the adoption of location-based services: The role of trust and perceived privacy risk. *Association for Information Systems - 26th International Conference on Information Systems, ICIS 2005: Forever New Frontiers*, 897–910.

Yang, Q., Gong, X., Zhang, K. Z. K., Liu, H., & Lee, M. K. O. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management*, *52*, 102065. https://doi.org/10.1016/j.ijinfomgt.2019.102065

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, *16*(4), 53–90. https://doi.org/10.2753/JEC1086-4415160403

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License