

DOI: https://doi.org/10.48009/4_iis_2026_139

Conceptualizing internet privacy concern constructs for generative artificial intelligence: An analysis of CFIP, IUIPC, and related IPC models

Julie Allen, *Middle Georgia State University and Georgia Southern University*, julie.allen@mga.edu and ja23916@georgiasouthern.edu

Hayden Wimmer, *Georgia Southern University*, hwimmer@georgiasouthern.edu

Carl M. Rebman, Jr., *University of San Diego*, carlr@sandiego.edu

Abstract

Despite the rapid proliferation of Generative Artificial Intelligence (GenAI) technologies, persistent concerns surrounding privacy and security continue to shape user trust and adoption. Internet privacy concern (IPC)—an individual's apprehension regarding the collection, processing, storage, disclosure, and potential misuse of personal information by websites, online services, organizations, or other users—has long served as a foundational construct across a broad range of empirical domains, including e-commerce, digital banking, and web-based data collection. This study evaluates five prominent IPC scales—Koohang et al. (2021), Van Slyke et al. (2006), the first- and second-order Internet Users' Information Privacy Concerns (IUIPC) models of Malhotra et al. (2004), and the Concern for Information Privacy (CFIP) scale of Smith et al. (1996)—in conjunction with established trust frameworks, to explain behavioral intent to use GenAI. Models incorporating the Koohang et al. (2021) and Van Slyke et al. (2006) formulations demonstrated the strongest explanatory power for behavioral intent, accounting for 46.2% and 59.6% of variance, respectively. Across all specifications that included trust constructs, trust exhibited a statistically significant positive relationship with behavioral intent, suggesting that trust may play a more central role than privacy concern alone in shaping user willingness to adopt GenAI systems. Beyond its substantive contribution to the emerging literature on GenAI adoption, privacy perception, and trust formation, this study's principal contribution is methodological: an SEM-based comparative framework for assessing the applicability, transferability, and limitations of established IPC measurement scales when extended to novel technologies, offering researchers empirically grounded guidance for scale selection in future privacy and trust research.

Keywords: generative artificial intelligence (Gen AI), privacy concerns, IUIPC, CFIP, trust, behavioral intent

Introduction

This study examines Generative Artificial Intelligence (GenAI) perceptions and behavioral intent based on privacy and security concerns, trust, risk, awareness, and related variables. It analyzes how existing privacy related models translate to and inform understanding on the GenAI domain. These models include Concerns for Information Privacy (CFIP), Malhotra et al.'s (2004) "Internet Users' Information Privacy Concerns (IUIPC)," Van Slyke et al.'s (2006) concern for information privacy in online consumer purchasing, and

Koohang et al.'s (2021) Social Media privacy and security concerns, trust, and awareness. In Smith et al.'s 1996 paper on "Measuring Individuals' Concerns about Organizational Practices," they recommended that executive leadership and management provide guidance in information privacy decisions to reduce the likelihood of burdensome regulations. An interesting thought as organizations and countries face their own decision points on Generative AI's value weighed against risks, including data privacy concerns.

Researchers have turned to Information Privacy Concern (IPC) scales for decades, applying them across an expanding array of technological and organizational contexts. Yet the proliferation of available scales raises a practical question the literature has not fully resolved: which instrument, among the many available, best suits a given research problem? Answering this question—by clarifying the comparative strengths and limitations of existing IPC measures—can sharpen how researchers design surveys and interpret findings going forward.

Generative Artificial Intelligence (GenAI) presents a case in point. As a still-unfolding technological shift, GenAI's long-term social consequences remain difficult to forecast. Its adoption has nonetheless accelerated rapidly, driven by promised gains in efficiency, even as concerns about security and data privacy protections persist alongside it. These concerns carry real weight. Businesses and employers have strong incentives to encourage GenAI adoption, but inadequate privacy protections risk provoking more stringent regulatory intervention. GenAI developers, in turn, must weigh model development against privacy safeguards, and user perceptions of GenAI may offer a useful signal for where that balance should fall. Applying IPC scales to the GenAI context, then, is not merely an academic exercise—it stands to meaningfully extend the existing body of privacy research.

This study takes up that task, examining GenAI perceptions and behavioral intent alongside privacy and security concerns, trust, risk, awareness, and related constructs. Rather than treating any single privacy framework as authoritative, we ask how well several established models translate into the GenAI domain—and how they compare once applied there. Five scales anchor the analysis: Smith et al.'s (1996) Concern for Information Privacy (CFIP), Malhotra et al.'s (2004) Internet Users' Information Privacy Concerns (IUIPC) both first and second order, Van Slyke et al.'s (2006) framework for privacy concern in online consumer purchasing, and Koohang et al.'s (2021) model of social media privacy and security concerns, trust, and awareness. Smith et al. (1996), notably, urged executive leadership to take an active role in guiding information privacy decisions, arguing that doing so would reduce the likelihood of burdensome regulation down the line. That recommendation feels newly relevant. Organizations and governments alike now face comparable decisions about Generative AI, weighing its promised value against its risks—data privacy chief among them.

Literature Review

Studies on privacy concerns focus across different technologies. Koohang et al. (2022) examined social media and whether Privacy Concerns or Security Concerns were more predictive of Trust or Awareness. Privacy Concerns and Security Concerns were significant on Trust and Awareness in two respective models in the Social Media domain, with Privacy Concerns as the most influential. Their findings support the importance of Social Media Awareness training by organizations to safeguard against privacy and security threats, and one of the future study recommendations was to evaluate other dependent variables like behavior. The original instrument for this paper came from Koohang et al. (2021) which developed and validated a measurement instrument for four constructs on social media privacy and security: privacy concerns, security, trust, and awareness.

Malhotra (2004) proposed a theoretical framework on Information Privacy Concerns for internet users based on traditional privacy constructs coupled with social theory, the importance of the trust-risk framework, and consideration of the reasoned-action paradigm (Malhotra et al., 2004, p. 337 & 340). While this study examines multiple privacy models including GIPC (Global Information Privacy Concerns), CFIP (Concerns for Information Privacy), and UIIPC (Internet Users Information Privacy Concerns), (Malhotra et al., 2004, p. 344) the proposed UIIPC with first order privacy constructs causal model and UIIPC with first order privacy constructs plus second order constructs on behavioral intent are the models we chose for this study (Malhotra et al., 2004, p. 349). The first order construct model is a 10-item UIIPC model based on Privacy Collection, Control, and Awareness, and the 2nd model consists of the same 10-item UIIPC construct plus second order Trust Beliefs and Risk Beliefs. Trust was identified as a mitigating factor in Risk concerns and reluctance to release personal information with the conclusion that privacy concerns negatively influence a user's willingness to transact (Malhotra et al., 2004, pp. 350-351).

However, not all studies reported those same findings. Van Slyke et al. (2006) sought to go beyond Technology Adoption Models that studied Trust on adoption and consider the oft-cited concern of information privacy on e-commerce adoption. They found that information privacy concerns, including Collection, Improper Access, Errors, and Secondary Usage, affected Risk Perceptions, Trust, and willingness to transact for a well-known company, though not for an unfamiliar one (Van Slyke et al., 2006, p. 415). Essentially, they studied CFIP as an antecedent of Trust and Risk. An important finding is that CFIP only indirectly affected willingness to transact and that Familiarity, Trust, and Risk Perceptions were more important (Van Slyke et al., 2006, p. 416). Nonetheless, CFIP seemed to be more important when the e-merchant was well known. Under some conditions, CFIP seemed to influence Trust, but this was not consistently found in their studies (Van Slyke et al., 2006, p. 437).

Unlike Van Slyke et al.'s study that evaluated CFIP, Trust, Risk, and Familiarity on Willingness to Transact, the foundational paper for CFIP by Smith et al. (1996) focused strictly on Privacy Concerns. In fact, in the abstract, they identified information privacy "as one of the most important ethical issues of the information age" (Smith et al., 1996). To the end of developing and validating a measurement instrument for information privacy concerns, they identified a 15-question instrument with four constructs: Collection, Errors, Unauthorized Secondary Use, and Improper Access. One of the recommendations from the study was the importance of executive leadership and management providing guidance in information privacy decisions to reduce the likelihood of burdensome regulations (Smith et al., 1996). An interesting thought as the United States faces its own decision points on Generative AI's value weighed against risks, including data privacy concerns.

Methods

Our paper applies these privacy concern models to Generative AI perceptions. They each have their own focus with Koochang et al.'s (2022) social media focus. While Smith et al.'s (1996) CFIP responds to important ethical concerns about information privacy but is not specific to online transactions. Malhotra et al. (2004) focused on digital transactions, specifically e-commerce. Van Slyke et al. (2006) considered privacy as an antecedent of Trust and Risk, while identifying Familiarity as a significant variable.

A survey about Generative Artificial Intelligence perceptions was generated in Qualtrics and administered through Amazon Mechanical Turk. Generative AI was defined, and well-known models were mentioned as examples. 52 total valid responses were captured. Respondents were paid a standard survey fee. The survey incorporated the entire instrument from Koochang et al. (2021) and Smith et al. (1996) (CFIP.) UIIPC, first and second order, from Malhotra et al.'s (2004) and Van Slyke et al.'s (2006) instruments were

included. Van Slyke's Risk Perception questions related to buying a product from a retailer are not included. Venkatesh et al.'s (2003) Attitude Toward Use and Behavioral Intent were used instead of Malhotra's Intent to Give Information and Van Slyke's Willingness to Transact. SmartPLS is used to analyze structural equation models in a reflective-formative model.

In order to evaluate IPC scales, we employ techniques including factor loading, construct reliability, discriminate validity, coefficient of determination, and multicollinearity. This work is not intended to claim any particular scale is superior but to review the aforesaid statistical analysis and infer the positives and negatives of the scales in comparison.

Research Questions

Research questions that inform our analysis include:

RQ1: *How does each privacy model perform on the Generative Artificial Intelligence domain based on Factor Analysis and Loading, Construct Reliability, and Discriminate Validity?*

RQ2: *How does each privacy model perform on the Generative Artificial Intelligence domain based on Coefficient of Determination, VIF, and Correlation?*

RQ3: *Which construct drives variance across the models?*

Results

This section presents a series of tables that represent the performance of each of the IPC models on generating AI. Table 1 presents the latent variables measuring GenAI perceptions loaded onto their corresponding construct appropriately except SecCon1, which loaded at .676, just below the .7 threshold for convergent validity; however, the AVE is still in acceptable range.

Table 1. Koohang on GenAI - Factor Analysis and Loading

	BI1	BI2	BI3	Priv Con1	Priv Con2	Priv Con3	Priv Con4	Sec Aware1	Sec Aware2	Sec Aware3	Sec Con1	Sec Con2	Sec Con3	Sec Con4	Sec Con5	Trust1	Trust2	Trust3
BI	0.99	0.98	0.98															
PrivCon				0.83	0.8	0.74	0.97											
SecAwareness								0.939	0.943	0.791								
SecConcerns											0.676	0.946	0.82	0.72	0.91			
Trust																0.966	0.908	0.923

Table 2 presents the latent variables measuring GenAI perceptions loaded onto their corresponding construct appropriately above the .7 threshold.

Table 2. Van Slyke on GenAI - Factor Analysis and Loading

Vankslyke Loading	BI1	BI2	BI3	Collect1	Collect2	Collect3	Collect4	Errors1	Errors2	Errors3	Errors4	Familiarity1	Familiarity2	Imp Access	Imp Access	Imp Access	Second ary1	Second ary2	Second ary3	Second ary4	Trust1	Trust2	Trust3	Trust4	Trust5	Trust6	Trust7
BI	0.985	0.981	0.977																								
Collection				0.958	0.950	0.946	0.924																				
Errors								0.847	0.905	0.959	0.952																
Familiarity												0.732	0.938														
Trust														0.880	0.915	0.880											
Secondary																	0.862	0.866	0.711	0.916							
Trust																					0.853	0.842	0.878	0.870	0.838	0.894	0.783

Table 3 presents the latent variables measuring GenAI perceptions loaded onto their corresponding construct appropriately above a .7 threshold for Malhotra et al.'s (2004) 10-item IUIPC scale with Behavioral Intent (BI) from Venkatesh et al. (2003).

Table 3. IUIPC (first order) on GenAI - Factor Analysis and Loading

IUIPC	Q1-IUIPC Aware-Malh	Q2-IUIPC Aware-Malh	Q3-IUIPC Aware-Malh	BI1	BI2	BI3	1Collecti onVS	2Collectio nVS	3Collectio nVS	4Collecti onVS	Q1-IUIPC Control	Q2-IUIPC Control	Q3-IUIPC Control
Aware	0.897	0.970	0.785										
BI				0.982	0.980	0.980							
Collection							0.957	0.950	0.947	0.925			
Control											0.890	0.936	0.845

Table 4 presents, latent variables measuring GenAI perceptions loaded onto their corresponding construct appropriately above a .7 threshold for the 10-item IUIPC plus 2nd order Risk and Trust Beliefs model from Malhotra et al. (2004) with Behavioral Intent (BI) from Venkatesh et al. (2003). Risk5Malhotra is a negative number, -.769, reflecting its reverse wording, "I would feel safe giving the information to AI."

Table 4. IUIPC (second order) Malhotra on GenAI - Factor Analysis and Loading

IUIPC	Q1-IUIPC Aware-Malh	Q2-IUIPC Aware-Malh	Q3-IUIPC Aware-Malh	BI1	BI2	BI3	1CollectionVS	2CollectionVS	3CollectionVS	4CollectionVS	Q1-IUIPC Control	Q2-IUIPC Control	Q3-IUIPC Control	Risk1 Malhotra	Risk2 Malhotra	Risk3 Malhotra	Risk4 Malhotra	Risk5 Malhotra	TrstBelief Menard-1	TrstBelief Menard-2	TrstBelief Menard-3	TrstBelief Menard-4	TrstBelief Menard-5
Aware	0.896	0.971	0.782																				
BI				0.984	0.980	0.979																	
Collection							0.958	0.950	0.946	0.924													
Control											0.890	0.935	0.846										
Risk														0.879	0.884	0.89	0.806	0.769					
TrstBelief																			0.929	0.914	0.871	0.902	0.854

Table 5 presents latent variables measuring GenAI perceptions loaded onto their corresponding construct appropriately above a .7 threshold.

Table 5. CFIP on GenAI - Factor Analysis and Loading

	BI1	BI2	BI3	Collection1	Collection2	Collection3	Collection4	Errors1	Errors2	Errors3	Errors4	Imp Access1	Imp Access2	Imp Access3	Secondary 1	Secondary 2	Secondary 3	Secondary 4
BI	0.982	0.979	0.982															
Collection				0.957	0.950	0.947	0.924											
Errors								0.849	0.904	0.960	0.952							
ImpAccess												0.881	0.916	0.879				
Secondary															0.862	0.865	0.716	0.916

Construct Reliability

The following tables reveal the construct reliability of the different models. In Table 6, AVE is greater than the .5 threshold and Cronbach's alpha, rho_a, and rho_c are equal to or greater than the .7 threshold, except for SecConcerns' rho_a which is -.479 and PrivConc at 1.583. These values fall outside of the theoretically valid range of [0,1]. SecCon1 loaded below the minimum threshold in Factor analysis which may contribute to the rho_a (Hair & Alamer, 2022). VIF value analysis, as suggested in Hair and Alamer (2022), suggest serious collinearity issues for PrivCon1 and PrivyConc2. Furthermore, Dijkstra-Henseler's rho (rho_a) can't theoretically exceed 1 or be negative indicating a Heywood case which is related to near-collinear indicators, or a function of the small sample size.

Table 6. Koohang et al. on GenAI – Construct Reliability

Construct Reliability				
	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
BI	0.980	0.981	0.987	0.962
PrivConc	0.900	1.583	0.904	0.705
SecAwareness	0.873	0.914	0.922	0.798
SecConcerns	0.951	-0.479	0.910	0.674
Trust	0.925	0.938	0.952	0.870

In Table 7, AVE is greater than .5 and Cronbach's alpha, rho_a, and rho_c are equal to or greater than the 0.7 threshold on all constructs except for Familiarity. Notably, Errors rho_a is 1.112 which is out of range, though loading does not exceed the threshold, VIF analysis, as suggested in Hair and Alamer (2022), indicates serious collinearity issues. With that said, rho_c and AVE are both within threshold.

Table 7. Van Slyke et al. on GenAI – Construct Reliability

Construct Reliability				
	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
BI	0.98	0.982	0.987	0.962
Collection	0.964	0.972	0.971	0.892
Errors	0.942	1.112	0.955	0.841
Familiarity	0.621	0.819	0.827	0.708
ImpAccess	0.876	0.925	0.921	0.795
Secondary	0.867	0.915	0.907	0.710
Trust	0.937	0.943	0.949	0.726

In Table 8, AVE is greater than .5 and Cronbach's alpha, rho_a, and rho_c are equal to or greater than the .7 threshold. Notably, Awareness rho_a is 1.345 which is outside of the valid range which indicates Heywood-case.

Table 8. IUIPC (first order) Malhotra on GenAI – Construct Reliability

Construct Reliability				
	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Aware	0.876	1.345	0.917	0.787
BI	0.98	1	0.987	0.962
Collection	0.964	0.975	0.971	0.893
Control	0.871	0.911	0.92	0.794

In Table 9, AVE is greater than .5 and Cronbach's alpha, rho_a, and rho_c are equal to or greater than the .7 threshold on all constructs except for Risk. Notably, Awareness rho_a is 1.369 which is out of range. Again, this could be sample size related and something researchers need to consider. Aware presents an

issue with out-of-range values; however, this construct is repeated between IUIPC first and second order so it would be expected.

Table 9. IUIPC (second order) Malhotra on GenAI – Construct Reliability

Construct Reliability				
	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Aware	0.876	1.369	0.916	0.786
BI	0.980	0.982	0.987	0.962
Collection	0.964	0.971	0.971	0.892
Control	0.871	0.910	0.920	0.794
Risk	0.910	0.978	0.927	0.718
TrstBelief	0.937	0.944	0.952	0.800

In Table 10, AVE is greater than .5 and Cronbach's alpha, rho_a, and rho_c are equal to or greater than the 0.7 threshold on all constructs except for Risk. Notably, BI and Errors rho_a are 1.021 and 1.11 which are out of range. Again, this construct is repeated in other models so we expect similar results for this construct between models.

Table 10. CFIP on GenAI – Construct Reliability

Construct Reliability				
	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
BI	0.980	1.021	0.987	0.962
Collection	0.964	0.972	0.971	0.892
Errors	0.942	1.11	0.955	0.842
ImpAccess	0.876	0.922	0.921	0.796
Secondary	0.867	0.913	0.907	0.710

Discriminant Validity

The following tables present the discriminant validity on the constructs and the different models. In Table 11, Discriminant Validity is established between all constructs based on HTMT and Fornell-Larcker metrics.

Table 11. Koohang et al. on GenAI – Discriminant Validity: HTMT and Fornell-Larcker Results

	HTMT Discriminant Validity				Fornell-Larcker Criterion				
	BI	Privacy Concerns	Security Awareness	Security Concerns	BI	Privacy Concerns	Security Awareness	Security Concern	Trust
BI					0.981				
PrivCon	0.096				0.162	0.840			
SecAware	0.254	0.364			0.239	0.205	0.894		
SecCon	0.049	0.633	0.360		-0.119	0.485	0.213	0.821	
Trust	0.593	0.263	0.152	0.163	0.571	-0.184	0.114	-0.123	0.933

In Table 12, Discriminant Validity was violated between Secondary Use and Improper access with their high HTMT value of .992. It is established for the other constructs. Given the value 0.992 is basically 1, this indicates ImpAccess and Secondary are statistically indistinguishable which is a clear violation of discriminant validity.

Table 12. Van Slyke et al. on GenAI – Discriminant Validity: HTMT and Fornell-Larcker Results

	HTMT Discriminant Validity						Fornell-Larcker Criterion						
	BI	Collection	Errors	Familiarity	Improper Access	Secondary Use	BI	Collection	Errors	Familiarity	Improper Access	Secondary Use	Trust
BI							0.981						
Collection	0.056						0.064	0.945					
Errors	0.129	0.308					0.150	0.290	0.917				
Familiarity	0.460	0.273	0.103				0.390	0.206	0.023	0.841			
ImpAccess	0.236	0.669	0.650	0.093			0.231	0.602	0.577	0.015	0.892		
Secondary	0.232	0.679	0.507	0.105	0.992		0.229	0.573	0.459	-0.013	0.848	0.842	
Trust	0.732	0.185	0.147	0.301	0.147	0.181	0.712	-0.163	0.017	0.235	0.061	0.120	0.852

In Table 13, Discriminant Validity is established for all constructs.

Table 13. IUIPC – first order Malhotra Heterotrait-Monotrait Ratio and Fornell-Larcker Criterion

	HTMT Discriminant Validity			Fornell-Larcker Criterion			
	Awareness	BI	Collection	Awareness	BI	Collection	Control
Aware				0.887			
BI	0.220			0.255	0.981		
Collection	0.751	0.056		0.666	0.063	0.945	
Control	0.724	0.172	0.681	0.678	0.161	0.611	0.891

In Table 14, Discriminant Validity is established for all constructs.

Table 14. IUIPC-second order Malhotra Heterotrait-Monotrait Ratio and Fornell-Larcker Criterion

	HTMT Discriminant Validity					Fornell-Larcker Criterion					
	Aware	BI	Collection	Control	Risk	Aware	BI	Collection	Control	Risk	TrustBelief
Aware						0.887					
BI	0.220					0.253	0.981				
Collection	0.751	0.056				0.665	0.063	0.945			
Control	0.724	0.172	0.681			0.679	0.162	0.611	0.891		
Risk	0.390	0.328	0.344	0.246		0.273	-0.368	0.296	0.209	0.847	
TrstBelief	0.198	0.530	0.238	0.136	0.621	-0.143	0.514	-0.216	-0.050	-0.604	0.894

In Table 15, Discriminant Validity is not established between Secondary Use and Improper access with their high HTMT value of 0.992. It is established for the other constructs. As in the VanSlyke scale, the HTMT shows the 2 constructs are indistinguishable statistically. These constructs are present in both scales so one would expect to see them recurring among models.

Table 15. CFIP Heterotrait-Monotrait Ratio and Fornell-Larcker Criterion

	HTMT Discriminant Validity				Fornell-Larcker Criterion				
	BI	Collection	Errors	Improper Access	BI	Collection	Errors	Improper Access	Secondary Use
BI					0.981				
Collection	0.056				0.063	0.945			
Errors	0.129	0.308			0.153	0.289	0.917		
ImpAccess	0.236	0.669	0.650		0.236	0.602	0.577	0.892	
Secondary	0.232	0.679	0.507	0.992	0.235	0.575	0.460	0.849	0.843

Coefficient of Determination

The following sections presents the results of the different models.

Koohang et al. on GenAI

Koohang et al.'s (2021) model (Privacy Concern, Security Concerns, Trust, and Awareness) adapted to GenAI, accounts for 46.2% of the variation in Behavioral Intent, the dependent variable, (Venkatesh et al., 2003) based on an R-squared of 0.462. The adjusted R Squared of 0.416 suggests an absence of overfitting (Llaudet & Imai, 2023); (Hair & Alamer, 2022).

Van Slyke et al. on GenAI

Van Slyke et al.'s (2006) model which includes the privacy related constructs of Collection, Errors, Improper Access, and Secondary Use along with Familiarity (adapted to GenAI) and Trust on Behavioral Intent (Venkatesh et al., 2003) has an R-squared of 0.596, which indicates the model explains 59.6% of the variation in the dependent variable BI and has moderate explanatory power, according to Hair et al. (2022). The adjusted R Squared of 0.542 suggests an absence of overfitting (Llaudet & Imai, 2023).

IUIPC-first order Malhotra on GenAI

Malhotra et al.'s (2004) 10-item IUIPC scale which includes the privacy related constructs of Collection and Control along with Awareness on Behavioral Intent (Venkatesh et al., 2003) on Generative Artificial Intelligence has an R-squared of 0.086, which indicates the model has no meaningful explanatory power. Adjusted R Squared is 0.029.

IUIPC-second order Malhotra on GenAI

However, Malhotra et al.'s (2004) 10-item IUIPC scale with Risk and Trust Beliefs reflects a R-squared of 0.399 and an adjusted R-squared of 0.334 indicating the increased predictive power of the model compared to the 10-item privacy focused scale without Risk and Trust Beliefs (Llaudet & Imai, 2023).

CFIP on GenAI

Similar to Malhotra et al.'s (2004) 10-item privacy scale, CFIP Collection, Errors, Improper Access, and Secondary Use privacy constructs on Behavioral Intent on Generative Artificial Intelligence has an R-squared of 0.073 and adjusted R Squared of -0.006 indicating no meaningful explanatory power.

Multicollinearity Analysis

The following tables present the multicollinearity analysis for the different models:

Table 16 presents findings that all constructs from Koohang et al. (2021) on GenAI are below the moderate threshold of .5. Venkatesh et al.'s (2003) BI does show moderate correlation with Koohang et al. (2021) Trust at .571.

Table 16. Koohang et al. on GenAI Correlation

	BI	PrivCon	Security Awareness	Security Concerns	Trust
BI	1				
PrivCon	0.162	1			
SecAware	0.239	0.205	1		
SecCon	-0.119	0.485	0.213	1	
Trust	0.571	-0.184	0.114	-0.123	1

In Table 17, of the independent variable questions, the VIF values for PrivCon1, PrivyConc2, SecCon3 and Trust1 exceed the critical threshold of 5 suggesting serious collinearity issues (Hair & Alamer, 2022).

Table 17. Koohang et al. on Gen AI VIF

	PrivCon-Koo -> BI	SecAwareness-Koo -> BI	SecConcerns-Koo -> BI	Trust-Koo -> BI
VIF	1.363	1.092	1.337	1.065

In Table 18, high Correlation is found in Improper Access and Secondary Use at .848 and BI and Trust at .712. Moderate correlation exists between multiple variables: Collection → Improper Access (ImpAccess), Collection → Secondary Use, and Errors → Improper Access

Table 18. Van Slyke et al. on GenAI Correlation

	BI	Collection VS	Errors VS	Familiarity VS	Improper Access VS	Secondary Use	Trust VS
BI	1						
Collection-VS	0.064	1					
Errors-VS	0.15	0.29	1				
Familiarity-VS	0.39	0.206	0.023	1			
ImpAccess-VS	0.231	0.602	0.577	0.015	1		
Secondary	0.229	0.573	0.459	-0.013	0.848	1	
Trust-VS	0.712	-0.163	0.017	0.235	0.061	0.12	1

In Table 19, of the independent variables, the Variable Inflation Factor values for Collection questions, Errors3, Errors4, and Trust3, and Trust4 exceed the critical threshold of 5 suggesting serious collinearity issues (Hair & Alamer, 2022). This is confirmed by the HTMT issues as described above.

Table 19. Van Slyke et al. on GenAI VIF

	Collection- VS -> BI	Errors- VS -> BI	Familiarity- VS -> BI	ImpAccess- VS -> BI	Secondary -> BI	Trust- VS -> BI
VIF	1.993	1.521	1.216	4.579	3.84	1.249

In Table 20, no constructs show high correlation above the .7 threshold. Moderate correlation exists between multiple variables: Awareness→ Collection, Awareness→ Control, and Control→ Collection.

Table 20. IUIPC – first order Malhotra on GenAI Correlation

	Aware	BI	Collection	Control
Aware	1			
BI	0.255	1		
Collection	0.666	0.063	1	
Control	0.678	0.161	0.611	1

In Table 21, out of the independent variables, the VIF values for Collection questions exceed the critical threshold of 5 suggesting serious collinearity issues (Hair & Alamer, 2022).

Table 21. IUIPC – first order Malhotra on GenAI VIF

	Aware - > BI	Collection -> BI	Control -> BI
VIF	2.277	1.964	2.022

In Table 22, No constructs show high correlation, although Awareness → Collection, Awareness → Control, Collection → Control, have a moderate, positive correlation, and Risk → TrustBeliefs have a moderate, negative correlation.

Table 22. IUIPC – second order Malhotra on GenAI Correlation

	Aware	BI	Collection	Control	Risk	TrstBelief
Aware	1					
BI	0.253	1				
Collection	0.665	0.063	1			
Control	0.679	0.162	0.611	1		
Risk	0.273	-0.368	0.296	0.209	1	
TrstBelief	-0.143	0.514	-0.216	-0.05	-0.604	1

In Table 23, of the independent variables in Malhotra's IUIPC plus Risk and Trust Beliefs, the following variables exceed the critical threshold of 5 suggesting serious collinearity issues: Collection (all questions), Risk2, and Risk3 (Hair & Alamer, 2022).

Table 23. IUIPC – second order Malhotra on GenAI VIF

	Aware - -> BI	Collection -> BI	Control -> BI	Risk -> BI	TrstBelief -> BI
VIF	2.298	2.04	2.065	1.685	1.617

In Table 24, Secondary Use and Improper Access show correlation at .849, above the .7 threshold. Moderate correlation exists between Collection → Improper Access, Collection → Secondary Use, Errors→ Improper access, Improper access → Collection

Table 24. CFIP on GenAI Correlation

	BI	Collection	Errors	Improper Access	Secondary Use
BI	1				
Collection	0.063	1			
Errors	0.153	0.289	1		
ImpAccess	0.236	0.602	0.577	1	0.
Secondary	0.235	0.575	0.46	0.849	1

In Table 25, of the independent variables, the VIF values for Collection (all questions), Errors3, and Errors4 exceed the critical threshold of 5 suggesting serious collinearity issues (Hair & Alamer, 2022).

Table 25. CFIP on GenAI VIF

	Collection -> BI	Errors -> BI	ImpAccess -> BI	Secondary -> BI
VIF	1.616	1.517	4.597	3.674

Path Coefficients- Relationship with BI

In Table 26, the Trust construct indicates significance on BI with a P value = 0.00

Table 26. Koohang et al. on GenAI Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
PrivCon -> BI	0.363	0.264	0.246	1.476	0.14
SecAware -> BI	0.153	0.197	0.164	0.928	0.353
SecCon -> BI	-0.255	-0.157	0.164	1.556	0.12
Trust -> BI	0.589	0.547	0.106	5.557	0

In Table 27, the Trust construct indicates significance on BI with a P value = 0.00

Table 27. Van Slyke et al. on GenAI Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
Collection-VS -> BI	0.02	-0.002	0.144	0.138	0.89
Errors-VS -> BI	0.039	0.018	0.153	0.252	0.801
Familiarity-VS -> BI	0.229	0.272	0.164	1.391	0.164
ImpAccess-VS -> BI	0.174	0.164	0.226	0.769	0.442
Secondary -> BI	-0.023	-0.023	0.189	0.121	0.904
Trust-VS -> BI	0.653	0.616	0.123	5.292	0

In Table 28, no constructs demonstrate significance on BI.

Table 28. IUIPC – first order Malhotra on GenAI Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
Aware -> BI	0.363	0.271	0.313	1.159	0.246
Collection -> BI	-0.202	-0.179	0.179	1.126	0.26
Control -> BI	0.038	0.053	0.174	0.221	0.825

In Table 29, the Trust construct indicates significance on BI with a P value = 0.034.

Table 29. IUIPC – second order Malhotra on GenAI Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
Aware -> BI	0.421	0.302	0.260	1.615	0.106
Collection -> BI	-0.04	-0.015	0.165	0.246	0.806
Control -> BI	-0.036	0.013	0.133	0.268	0.788
Risk -> BI	-0.194	-0.249	0.197	0.987	0.324
TrstBelief -> BI	0.447	0.406	0.210	2.122	0.034

In Table 30, no constructs demonstrate significance on BI.

Table 30. CFIP on GenAI Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
Collection -> BI	-0.138	-0.149	0.182	0.759	0.448
Errors -> BI	0.02	0.006	0.229	0.088	0.93
ImpAccess -> BI	0.172	0.165	0.27	0.636	0.525
Secondary -> BI	0.16	0.171	0.245	0.654	0.513

RQ1: *How does each privacy model perform on the Generative Artificial Intelligence domain based on Factor Analysis and Loading, Construct Reliability, and Discriminate Validity?*

While some issues could be related to the small sample size of our exploratory study, we note there are recurring issues between shared constructs. Out of range values and multicollinearity seem to be an issue that needs to be resolved in order to implement the scales on a larger study.

RQ2: *How does each privacy model perform on the Generative Artificial Intelligence domain based on Coefficient of Determination, VIF, and Correlation?*

Again, we note issues with multicollinearity as measured by VIF and correlation. The coefficient of determination, as measured as R^2 , was 0.469, 0.596, 0.086, 0.399, and 0.073 respectively illustrating the predictive power of the Koohang and VanSlyke scales outperform the remaining scales as measured by R^2 or R^2 Adjusted.

RQ3: *Which construct drives variance across the models?*

Koohang et al. (2021) drives variance across the models on behavioral intent to use GenAI. Koohang et al.'s (2021) and Van Slyke et al.'s (2006) models applied to Generative Artificial Intelligence had the most explanatory power, accounting for 46.2% and 59.6% of the variation respectively in Venkatesh et al.'s (2003) Behavioral Intent. It was notable that in all models that measured Trust, Trust is statistically significant on Behavioral Intent. In fact, it's the only variable that is, which is an important outcome of this analysis.

Limitations and Discussion

Limitations of the study include a small sample size of 52. Furthermore, more investigation needs to be made on the out of bounds issues that plagued many of the models. For research question 1, Factor Analysis and Loading for all models on Generative Artificial Intelligence were strong, though Construct Reliability suggests further investigation in general, and Discriminant Validity indicates investigation into the models of Van Slyke (2006) et al. and CFIP. For research question 2, Koohang et al.'s (2021) and Van Slyke et al.'s (2006) models applied to Generative Artificial Intelligence had the most explanatory power, accounting for 46.2% and 59.6% of the variation respectively in Venkatesh et al.'s (2003) Behavioral Intent.

Conclusion

Generative Artificial Intelligence (GenAI) is a technological evolution that has yet unknown impacts on our society. While adoption of this technology is widespread and promises efficiencies, there are concerns surrounding it, including security and data privacy protections. These concerns matter because adoption is important to business and employers, and failure to adequately protect user privacy could prompt stricter

regulatory responses. GenAI corporations may have to consider how to balance privacy concerns and consumer trust with AI model development. Users' GenAI perceptions from our survey identify models and variables that may support future research.

This study examined Generative Artificial Intelligence perceptions and behavioral intent based on privacy and security concerns, trust, risk, awareness, and related variables. It analyzed how existing models may inform understanding about the GenAI domain. These models include Concerns for Information Privacy (CFIP), Malhotra et al.'s (2004) "Internet Users' Information Privacy Concerns (IUIPC)," Van Slyke et al.'s (2006) concern for information privacy in online consumer purchasing, and Koohang et al.'s (2022) Social Media privacy and security concerns, trust, and awareness. Koohang et al.'s (2021) and Van Slyke et al.'s (2006) models applied to Generative Artificial Intelligence had the most explanatory power, accounting for 46.2% and 59.6% of the variation respectively in Venkatesh et al.'s (2003) Behavioral Intent. It was notable that in all models that measured Trust, Trust was statistically significant on Behavioral Intent.

References

- Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics*, 1(3), 100027. <https://doi.org/10.1016/j.rmal.2022.100027>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. 3rd ed. Sage. <https://uk.sagepub.com/en-gb/eur/a-primer-on-partial-least-squares-structural-equation-modeling-pls-sem/book270548>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 115-135. <https://doi.org/10.1007/s11747-014-0403-8>
- Koohang, A., Floyd, K., Yerby, J., & Paliszkievicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. *Issues in Information Systems*, 22(2), 133-145.
- Koohang, A., Nord, J., Floyd, K., & Paliszkievicz, J. (2022). Social media privacy and security concerns: Trust and Awareness. *Issues in Information Systems*, 23(3), 253-264.
- Llaudet, E., & Imai, K. (2023). *Data Analysis for Social Science*. Princeton University Press.
- 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>
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS quarterly*, 20(2), 167-196.

Van Slyke, C., Shim, J. P., Johnson, R. D., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 415-447.

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.

Appendix: Survey Questions

Koohang et al. (2022)	
Koohang et al. 2021 Collection	I am concerned that AI are collecting my personal information.
Koohang et al. 2021 Secondary Usage	I am concerned that AI share/sell my stored personal information in their databases to other companies
Koohang et al. 2021 Improper Access	I am concerned that AI do not devote enough time and effort to preventing unauthorized access to my personal information.
Koohang et al. 2021 Control	It bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by AI.
Koohang et al. 2021 Awareness Construct Q1	When using AI, I am aware of the potential security threats and risks and their negative consequences.
Koohang et al. 2021 Awareness Construct Q2	When using AI, I am aware of potential privacy threats and risks and their negative consequences.
Koohang et al. 2021 Awareness Construct Q3	When using AI, I am aware that there is potential for harm/loss associated with my security and privacy.
Koohang et al. 2021 Security Concerns Construct Q1	When I'm on AI sites, I'm concerned about: Identity theft (attacker stealing my personal information) (1)
Koohang et al. 2021 Security Concerns Construct Q2	When I'm on AI sites, I'm concerned about: Impersonation/Social phishing (attacker impersonating a real person through a fake website to steal my data, including login credentials and credit card numbers, etc.). (2)
Koohang et al. 2021 Security Concerns Construct Q3	When I'm on AI sites, I'm concerned about: Hijacking (attacker taking control over my profile). (3)
Koohang et al. 2021 Security Concerns Construct Q4	When I'm on AI sites, I'm concerned about: Image retrieval and analysis (attacker using face and image recognition software to find more information about me and my linked profiles). (4)
Koohang et al. 2021 Security Concerns Construct Q5	When I'm on AI sites, I'm concerned about: Malware attacks (attacker sending malware injected scripts or malicious software to perform activities on my device without my knowledge). (5)
Koohang et al. 2021 Trust Construct Q1	When it comes to privacy and security, the AI I use: are trustworthy (1)
Koohang et al. 2021 Trust Construct Q2	When it comes to privacy and security, the AI I use: keep my best interests and well-being in mind. (2)
Koohang et al. 2021 Trust Construct Q3	When it comes to privacy and security, the AI I use: are competent in protecting and safeguarding my personal information. (3)
Van Slyke et al. (2006)	
VanSlyke Collection Q1	It usually bothers me when companies ask me for personal information.

Issues in Information Systems

Volume 27, Issue 4, pp. 469-487, 2026

VanSlyke Collection Q2	When companies ask me for personal information, I sometimes think twice about providing it.
VanSlyke Collection Q3	It bothers me to give personal information to so many companies.
VanSlyke Collection Q4	I'm concerned that companies are collecting too much personal information about me.
VanSlyke Improper Access Q1	Companies should devote more time and effort to preventing unauthorized access to personal information.
VanSlyke Improper Access Q2	Companies should take more steps to make sure that unauthorized people cannot access personal information on their computer.
VanSlyke Improper Access Q3	AI Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
VanSlyke Errors Q1	All the personal information in AI computer databases should be double-checked for accuracy—no matter how much this costs.
VanSlyke Errors Q2	AI companies should have better procedures to correct errors in personal information.
VanSlyke Errors Q3	AI companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
VanSlyke Errors Q4	AI companies should take more steps to make sure that the personal information in their files is accurate.
VanSlyke Familiarity Q1	I am familiar with AI.
VanSlyke Familiarity Q2	I am familiar with inquiring about information and/or tasks from AI.
VanSlyke Trust Q1	Artificial Intelligence (AI) has the skills and expertise to perform transactions in an expected manner. (1)
VanSlyke Trust Q2	Artificial Intelligence (AI) has access to the information needed to handle transactions appropriately. (2)
VanSlyke Trust Q3	Artificial Intelligence (AI) is fair in its conduct of user transactions. (3)
VanSlyke Trust Q4	Artificial Intelligence (AI) is fair in its policies following a transaction. (4)
VanSlyke Trust Q5	Artificial Intelligence (AI) is open and receptive to user needs. (5)
VanSlyke Trust Q6	Artificial Intelligence (AI) makes good faith efforts to address most user concerns. (6)
VanSlyke Trust Q7	Artificial Intelligence (AI) is trustworthy. (7)
IUIPC - first order Malhotra et al. (2004)	
IUIPC Collection Q1	It usually bothers me when online companies ask me for personal information.
IUIPC Collection Q2	When online companies ask me for personal information, I sometimes think twice before providing it.
IUIPC Collection Q3	It bothers me to give personal information to so many online companies.
IUIPC Collection Q4	I'm concerned that online companies are collecting too much personal information about me.
IUIPC Control Q1	Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
IUIPC Control Q2	Consumer control of personal information lies at the heart of consumer privacy.
IUIPC Control Q3	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
IUIPC Awareness Q1	AI, seeking information online, should disclose the way the data are collected, processed, and used.
IUIPC Awareness Q2	A good consumer online privacy policy should have a clear and conspicuous disclosure.

IUIPC Awareness Q3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.
IUIPC - second order Malhotra et al. (2004) = IUIPC first order Malhotra et al. (2004) + second order Trust Beliefs and Risk Beliefs	
Risk1 Malhotra	Malhotra In general, it would be risky to give information to AI.
Risk2 Malhotra	There would be high potential for loss associated with giving information to AI.
Risk3 Malhotra	There would be too much uncertainty associated with giving information to AI.
Risk4 Malhotra	Providing AI with information would involve many unexpected problems.
Risk5 Malhotra	I would feel safe giving the information to AI.
TrustBelief Malhotra1	AI would be trustworthy in handling my data and input. (1)
TrustBelief Malhotra2	AI would tell the truth and fulfil promises related to data and input provided by me. (2)
TrustBelief Malhotra3	AI would keep my best interests in mind when dealing with my data and input. (3)
TrustBelief Malhotra4	AI are, in general, predictable and consistent regarding the usage of data and input. (4)
TrustBelief Malhotra5	AI are always honest with customers when it comes to using data and input that I would provide. (5)
CFIP Smith et al. (1996)	
CFIP = VanSlyke Collection Q1	It usually bothers me when companies ask me for personal information.
CFIP = VanSlyke Collection Q2	When companies ask me for personal information, I sometimes think twice about providing it.
CFIP = VanSlyke Collection Q3	It bothers me to give personal information to so many companies.
CFIP = VanSlyke Collection Q4	I'm concerned that companies are collecting too much personal information about me.
CFIP = VanSlyke Errors Q1	All the personal information in AI computer databases should be double-checked for accuracy—no matter how much this costs.
CFIP = VanSlyke Errors Q2	AI companies should have better procedures to correct errors in personal information.
CFIP = VanSlyke Errors Q3	AI companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
CFIP = VanSlyke Errors Q4	AI companies should take more steps to make sure that the personal information in their files is accurate.
CFIP = Van Slyke/IUIPC Secondary Usage Q1	AI should not use personal information for any purpose unless it has been authorized by the individuals who provided information.
CFIP = Van Slyke/IUIPC Secondary Usage Q2	When people give personal information to a AI for some reason, the AI should never use the information for any other reason.
CFIP = Van Slyke/IUIPC Secondary Usage Q3	AI should never sell the personal information in their computer databases to other companies.
CFIP = Van Slyke/IUIPC Secondary Usage Q4	AI should never share personal information with other companies unless it has been authorized by the individuals who provided the information
CFIP = VanSlyke Improper Access Q1	Companies should devote more time and effort to preventing unauthorized access to personal information.

CFIP = VanSlyke Improper Access Q2	Companies should take more steps to make sure that unauthorized people cannot access personal information on their computer.
CFIP = VanSlyke Improper Access Q3	AI Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
Venkatesh et al. (2003) Behavioral Intent (BI) and Attitude Toward Use (ATU)	
BI 1 Venkatesh	I intend to use AI.
BI 2 Venkatesh	I predict I would use AI.
BI 3 Venkatesh	I plan to use AI in the near future.
ATU 1 Venkatesh	I am comfortable using AI.
ATU 2 Venkatesh	Using AI is a wise idea
ATU 3 Venkatesh	I like the idea of using AI
ATU 4 Venkatesh	Using AI is pleasant