SSR Journal of Economics, Business and Management (SSRJEBM)

Homepage: https://ssrpublisher.com/ssrjebm/

Volume 3, Issue 3, 2026 ISSN: 3049-0405

From Privacy Concern to Strategic Resistance: A Dual-Pathway Model of Power-Enhancing Responses in Digital Banking

Truong Thi Minh Trang

Ho Chi Minh City University of Foreign Languages – Information Technology

Received: 20.01.2026 | **Accepted:** 24.02.2026 | **Published:** 07.03.2026

***Corresponding author:** Truong Thi Minh Trang

DOI: *10.5281/zenodo.18899060*

Abstract **Original Research Article**

This study investigates the psychological mechanisms through which information privacy concerns translate into power-enhancing responses—strategic consumer behaviors including information falsification, technological countermeasures deployment, and disclosure refusal—in digital banking contexts. Drawing on the Antecedent-Privacy Concern-Outcome (APCO) framework, Concern for Information Privacy (CFIP) theory, and Power-Responsibility Equilibrium perspective, we develop and test an integrated model specifying dual mediation pathways: an affective pathway through perceived data vulnerability and an evaluative pathway through negative attitudes toward information practices. Survey data from 251 active digital banking users in Vietnam were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). Results reveal that all four CFIP dimensions—Collection, Secondary Use, Unauthorized Access, and Errors—significantly predict overall privacy concern, with Errors concerns exhibiting the strongest effect ($\beta = 0.319$). The model explains 88.7% of variance in power-enhancing responses, demonstrating that privacy concerns operate through both direct cognitive pathways ($\beta = 0.326$) and indirect pathways via perceived vulnerability ($\beta = 0.379$) and negative attitudes ($\beta = 0.269$). Perceived vulnerability emerges as the critical affective mechanism, with overall concern strongly predicting vulnerability ($\beta = 0.577$), which then catalyzes defensive behaviors. These findings resolve the privacy paradox by demonstrating that privacy concerns predict consequential behaviors through sophisticated resistance mechanisms rather than simple disclosure decisions. The study contributes to privacy theory by specifying the psychological architecture linking cognitive concerns to behavioral outcomes and offers practical guidance for financial institutions seeking to prevent invisible data contamination through information falsification.

Keywords: Information privacy concern, Power-enhancing responses, Perceived vulnerability, Digital banking, Privacy paradox, Power-Responsibility Equilibrium.

1. INTRODUCTION

The digital transformation of financial services has fundamentally altered the relationship between consumers and banking institutions, creating unprecedented opportunities for personalized services while simultaneously exposing consumers to significant privacy risks

(Vives, 2019). Digital banking platforms now serve as primary touchpoints for millions of customers worldwide, systematically collecting vast amounts of sensitive personal and financial data to deliver seamless, customized experiences (Gomber et al., 2017). This data-intensive business model, however, has rendered financial institutions particularly vulnerable to security breaches

When consumers perceive their personal data as compromised or mismanaged by financial institutions, they do not simply accept vulnerability passively. Drawing on the Power-Responsibility Equilibrium (PRE) framework, research demonstrates that consumers engage in defensive actions to restore the power balance when they perceive that businesses and regulators have failed in their responsibility to protect consumer data (Lwin et al., 2007). The PRE framework posits that in relationships characterized by power asymmetry, the party holding greater power bears a corresponding responsibility to create an environment of trust and confidence. When this responsibility is abdicated—as occurs when organizations experience data breaches, engage in unauthorized data sharing, or demonstrate inadequate privacy protection—consumers attempt to reclaim power through various defensive mechanisms (Culnan & Armstrong, 1998; Pavlou & Gefen, 2004).

Among the various defensive responses available to consumers - including complete avoidance, service withdrawal, complaint behavior, and negative word-of-mouth, one category of behavior stands out as particularly consequential yet theoretically under-examined: *power-enhancing responses*. Power-enhancing responses represent strategic acts of consumer resistance designed to reclaim control over personal information in asymmetric power relationships (Acquisti & Brandimarte, 2015; Brunton & Nissenbaum, 2015). These behaviors include: (1) fabricating or falsifying personal information when Except for the cite references I've already attached, please provide me with references that are relevant and appropriate to the content above, and cite the paragraph that you deem suitable.required to provide data, (2) deploying technological countermeasures such as anonymizers, virtual private networks, or cookie rejection to disguise identity and origin, and (3) refusing outright to provide personal information or declining to complete transactions that require data disclosure (Lwin et al., 2007; Wirtz et al., 2007). Unlike passive avoidance strategies that merely involve disengagement from services, or post-hoc complaint mechanisms that signal dissatisfaction after the fact, power-enhancing responses constitute proactive, calculative strategies that allow consumers to maintain nominal participation in digital services while simultaneously undermining the accuracy, completeness, and reliability of the data ecosystem upon which these services depend.

Recent empirical evidence suggests that information falsification—a core component of power-enhancing responses—has become increasingly prevalent as a defensive reaction to perceived corporate overreach and vulnerability. Research indicates that consumers strategically provide intentionally inaccurate information when they lack trust in a company's data collection practices or perceive inadequate privacy protection (Chen et al., 2023; Martin et al., 2017). This behavior represents what legal scholars have termed "privacy self-defense"—conscious efforts by individuals to withhold, obfuscate, or fabricate personal data in response to perceived privacy threats (Brunton & Nissenbaum, 2015).

What makes power-enhancing responses particularly noteworthy from both theoretical and managerial perspectives is their insidious impact on business operations—an impact potentially more damaging than straightforward customer attrition. When customers leave a platform or service entirely through traditional churn mechanisms, firms can clearly observe the loss, implement retention strategies, or accept the departed customer as an unavoidable cost of doing business. The visibility of customer churn enables firms to measure its magnitude, identify its causes, and respond strategically. However, when customers remain nominally engaged but systematically provide false information, several critical problems emerge that operate below the surface of conventional business metrics. For example, falsified information creates operational inefficiencies as firms invest substantial resources marketing to non-existent customer segments, processing deliberately fraudulent applications, or making strategic decisions based on fundamentally distorted customer profiles (Goldfarb & Tucker, 2011; Japec et al., 2015).

Furthermore, power-enhancing responses represent a form of intelligent consumer resistance that reflects sophisticated risk calculations rather than mere privacy naivety or technological incompetence. Contemporary consumers are not simply trading privacy for convenience in straightforward cost-benefit analyses, nor are they exhibiting the kind of privacy carelessness sometimes attributed to them in popular discourse. Instead, they are engaging in strategic information management practices characterized by calculated selectivity: revealing accurate data in contexts perceived as trustworthy while deliberately falsifying information in contexts perceived as exploitative or inadequately protected (Acquisti & Brandimarte, 2015; Dienlin & Trepte, 2015). This pattern of behavior suggests that consumers maintain nuanced mental models of institutional trustworthiness and adjust their disclosure strategies accordingly based on assessments of vulnerability, anticipated consequences, and perceptions of power balance (Culnan & Armstrong, 1998). Such calculated resistance fundamentally challenges firms' assumptions about the social contract governing digital data collection, the meaning of user consent, and the sustainability of data-intensive business models built on assumptions of consumer transparency and compliance.

From the theoretical point of view, the phenomenon of consumer power-enhancing responses to privacy concerns presents several unresolved theoretical tensions that demand rigorous investigation. **First,** tension exists between the Privacy Paradox perspective—consumers express high privacy concerns yet readily disclose information, suggesting attitude-behavior disconnect (Barth & de Jong, 2017)—and the Power-Responsibility Equilibrium framework predicting that perceived power imbalances trigger strategic resistance through falsification, technological obfuscation, and selective refusal (Lwin et al., 2007). This creates fundamental confusion: do privacy concerns predict consequential behaviors or remain performative attitudes? **Second**, substantial ambiguity exists regarding psychological mechanisms converting cognitive concerns into behavioral responses. The APCO model establishes privacy concern as central mediator but underspecifies transformation processes (H. Smith et al., 2011a). (Martin et al., 2017) introduced perceived vulnerability as critical affective mechanism mediating concern-behavior relationships, yet the relationship between cognitive concern and affective vulnerability remains theoretically underspecified and empirically unexamined.

Third, inconsistencies exist regarding which CFIP dimensions—Collection, Secondary Use, Unauthorized Access, Errors —most strongly predict defensive responses. Research has not established whether dimensions exert differential effects, operate independently or synergistically, or manifest effects directly versus through mediating mechanisms like vulnerability and negative attitudes (Malhotra et al., 2004). **Fourth**, theoretical ambiguity exists about attitudinal mechanisms' role. While privacy concern represents cognitive risk assessment, attitudes toward information practices capture evaluative fairness judgments. Research has not clarified whether attitudes represent independent pathways to power-enhancing responses or interact with cognitive and affective mechanisms, nor specified the sequential ordering among concern, vulnerability, and attitudes in determining behaviors (Culnan & Armstrong, 1998).

These theoretical tensions are not merely academic curiosities without practical import. They carry profound implications for both theory development and managerial practice. If the privacy paradox perspective accurately characterizes consumer behavior, organizations can reasonably pursue aggressive data collection strategies with minimal concern for privacy objections, secure in the knowledge that stated concerns will not materialize into behavioral resistance. However, if the Power-Responsibility Equilibrium framework better captures reality, organizations face a critical threat operating beneath the surface of conventional business metrics: consumers who appear engaged and compliant are actually contaminating organizational data ecosystems through systematic information falsification, rendering business intelligence unreliable, predictive models inaccurate, and strategic decisions fundamentally misguided. Resolving these theoretical tensions therefore carries direct implications for organizational strategy, privacy policy design, and regulatory approaches (Goldfarb & Tucker, 2011).

This study addresses these theoretical tensions by developing and empirically testing a comprehensive model that integrates the four CFIP dimensions (Collection, Secondary Use, Unauthorized Access, Errors), overall concern for information privacy, perceived data vulnerability, attitudes toward information practices (negative), and power-enhancing responses within a unified theoretical framework grounded in the APCO model (H. Smith et al., 2011b) and Power-Responsibility Equilibrium perspective (Lwin et al., 2007).By examining both direct pathways and indirect pathways through multiple mediators, the research clarifies the psychological architecture linking privacy concern antecedents to behavioral outcomes. The study provides empirical resolution to the tension between the privacy paradox perspective and evidence of consequential defensive behaviors by demonstrating conditions under which privacy concerns translate into meaningful resistance. Furthermore, by situating the analysis within the high-stakes context of digital banking—where privacy violations through data breaches are frequent, consequential, and highly visible—the study offers empirical evidence under conditions where theoretical predictions should be most pronounced and managerial implications most salient.

To achieve these research objectives, the study addresses the following specific research questions:

How do the direct and indirect pathways from privacy concern dimensions through overall concern, vulnerability perceptions, and negative attitudes combine to create an integrated explanation of power-enhancing responses?

The remainder of this thesis is organized as follows. Chapter 2 reviews relevant literature on information privacy concerns, the CFIP dimensions, perceived data vulnerability, attitudes toward information practices, power-enhancing responses, and the theoretical frameworks that inform this research including the APCO model, CFIP theory, Power-Responsibility Equilibrium perspective, and Gossip Theory. Chapter 3 develops the theoretical model and articulates specific research hypotheses linking the constructs. Chapter 4 describes the research methodology including research design, sample selection, measurement instrument development, data collection procedures, and planned data analysis techniques. Chapter 5 presents the results of empirical analysis including measurement model assessment and structural model testing. Chapter 6 discusses the findings, articulates theoretical and practical implications, acknowledges limitations, and identifies directions for future research.

2. THEORETICAL FRAMEWORK

2.1 The APCO Framework: Organizing Privacy Research

Privacy research suffers from theoretical fragmentation. The APCO model (Antecedents → Privacy Concerns → Outcomes) provides organizing structure (H. Smith et al., 2011b). The logic is straightforward: various antecedent factors trigger privacy concerns, which then generate behavioral and attitudinal outcomes. This sequential architecture matters because it identifies privacy concern as the central mediating mechanism—the psychological state that translates contextual factors into consequential responses (Malhotra et al., 2004).

Three implications follow. First, privacy concern operates as a mediator, not merely a correlate. Antecedents do not directly cause behaviors; they work through the psychological mechanism of concern (Dinev & Hart, 2006). Second, the model predicts that strengthening privacy concern amplifies its behavioral effects. Consumers experiencing intense concern should exhibit stronger defensive responses. Third, the framework implies that interventions targeting concern antecedents can indirectly influence outcomes by modulating the intensity of concern itself.

However, the APCO framework underspecifies the psychological processes linking concern to behavior. It establishes that concern mediates, but not how. Cognitive privacy risk assessments must transform into action through intermediate psychological states. This study addresses this specification gap by incorporating perceived vulnerability as an affective mechanism and attitudes toward information practices as an evaluative mechanism. Both constructs represent psychological pathways through which concern translates into power-enhancing responses.

2.2 Concern for Information Privacy: The Four-Dimensional Structure

Privacy concern is not unidimensional. The CFIP framework establishes four distinct facets (H. J. Smith et al., 1996).Collection (concerns about data gathering volume and scope), Secondary Use (worries about purpose limitation violations), Unauthorized Access (fears of security breaches), and Errors (concerns about data accuracy and correction mechanisms). This dimensional structure matters theoretically because different privacy threats activate different psychological mechanisms and may predict distinct behavioral responses (Malhotra et al., 2004).

The four dimensions reflect distinct failure modes in organizational data management. Collection concerns arise when firms gather excessive data beyond what transactions require. Secondary Use concerns emerge when firms repurpose data beyond original consent boundaries. Unauthorized Access concerns activate when security controls fail. Errors concerns surface when data quality degrades and correction mechanisms prove inadequate. Each dimension represents a different way organizations can violate consumer privacy expectations (Culnan & Armstrong, 1998; H. J. Smith et al., 1996).

This dimensional decomposition creates analytical leverage. Rather than treating privacy concern as a homogeneous construct, we can test whether specific dimensions exert differential effects (Belanger & Crossler, 2011). Do all four dimensions equally predict power-enhancing responses, or do certain dimensions (e.g., Unauthorized Access following data breaches) dominate? Do dimensions operate independently through separate pathways, or do they converge through common mediating mechanisms? These questions require dimensional analysis rather than aggregate measurement.

2.3 Power-Responsibility Equilibrium: The Theoretical Foundation for Defensive Responses

Asymmetric power relationships impose corresponding responsibilities on power holders (Lwin et al., 2007). The PRE framework posits that parties possessing superior power—whether through information advantages, resource control, or institutional authority—bear responsibility to create trust and protect vulnerable parties. When power holders abdicate this responsibility through negligence, exploitation, or incompetence, the resulting imbalance triggers defensive responses from subordinate parties aimed at restoring equilibrium (Lwin et al., 2007; Steindl et al., 2015).

In digital banking, firms hold structural power advantages. They control transaction platforms, dictate data collection terms, design privacy policies unilaterally, and leverage information asymmetries about data usage practices (Culnan & Armstrong, 1998; Pavlou & Gefen, 2004). This power concentration creates responsibility: firms must protect consumer data, respect privacy boundaries, and deploy data only within consent limits. Data breaches, unauthorized sharing, and inadequate security represent responsibility failures—instances where firms with superior power failed to safeguard consumer interests.

PRE theory predicts specific consequences for responsibility failures (Rosenau, 1984). Consumers do not passively accept vulnerability. Instead, they engage in power-enhancing responses designed to restore balance: providing false information to corrupt firm data systems, deploying technological countermeasures to obstruct surveillance, and refusing data disclosure to reclaim informational control. These behaviors represent rational strategic responses to perceived exploitation, not mere privacy neurosis. Consumers recognize power imbalances and act deliberately to rebalance relationships through available resistance mechanisms (Casciaro et al., 1611).

2.4 Perceived Data Vulnerability: The Affective Mechanism

Privacy concern represents cognitive risk assessment—a calculated judgment about probability and magnitude of privacy threats. Perceived vulnerability represents affective response—a felt state of personal susceptibility and insecurity (Martin et al., 2017). This distinction matters because cognitive assessments do not automatically generate behavioral action. Individuals can intellectually recognize risks while remaining emotionally unaffected, producing the well-documented privacy paradox where expressed concerns fail to predict behavior (Dimodugno et al., 2021; Kim et al., 2023).

Gossip theory provides the theoretical foundation for vulnerability's mediating role. When individuals perceive that others possess sensitive personal information, they experience vulnerability because that information enables reputational damage through gossip—unauthorized sharing of private details that undermines social standing (Martin et al., 2017). Vulnerability emerges from loss of narrative control: others can now construct and disseminate stories about the individual without permission or oversight. This loss of control over one's social narrative creates anxiety, insecurity, and felt exposure (Palmer, 2007).

The mechanism operates as follows. Privacy concerns identify potential threats to informational control (Kim et al., 2023). When these threats materialize—through data breaches, unauthorized access, or perceived exploitation—cognitive concern intensifies into affective vulnerability. This emotional transformation activates defensive motivations. Individuals experiencing vulnerability seek to regain control through available means, including information falsification, technological obfuscation, and disclosure refusal. Vulnerability thus serves as the psychological bridge converting cognitive risk assessments into emotionally-driven protective actions (Kim et al., 2023; Palmer, 2007).

This theoretical architecture resolves the privacy paradox (Kokolakis, 2015). Concerns alone prove insufficient to motivate action because they remain abstract cognitive states. However, when concerns generate felt vulnerability—personal anxiety about exposure and exploitation—the emotional salience catalyzes behavioral response. The paradox dissolves when we recognize that behavioral prediction requires affective activation, not merely cognitive acknowledgment of risk (Barth & de Jong, 2017; Dienlin & Trepte, 2015).

2.5 Attitudes toward Information Practices: The Evaluative Mechanism

Attitudes toward information practices capture evaluative judgments about the appropriateness, fairness, and acceptability of organizational data management behaviors (Ajzen, 1991). While privacy concern assesses risk magnitude and vulnerability reflects affective anxiety, attitudes embody normative evaluations: whether firms' data practices deserve approval or condemnation based on fairness criteria (Palmer, 2007; Wirtz et al., 2007).

These evaluative judgments operate through distinct psychological pathways. Privacy calculus theory demonstrates that individuals weigh perceived risks against anticipated benefits when deciding whether to disclose information (Dinev & Hart, 2006). However, this cost-benefit calculation embeds fairness assessments: even when benefits exceed risks, individuals may resist disclosure if they judge the exchange fundamentally unfair. Attitudes toward information practices capture this fairness dimension—whether organizations demonstrate respect for consumer autonomy, transparency in daxta usage, and restraint in collection practices.

Negative attitudes trigger resistance for three reasons (Schrader & Lawless, 2004). First, they signal normative violations. When consumers judge organizational practices as exploitative or disrespectful, they experience moral objection beyond mere risk aversion. Second, negative attitudes reduce perceived legitimacy. Consumers question whether firms deserve the data access they demand when practices appear unfair. Third, attitudes shape reciprocity norms. Consumers who perceive organizational exploitation feel justified in responding with countermeasures including information falsification—restoring fairness through strategic resistance.

The theoretical contribution lies in recognizing attitudes as an independent pathway from privacy concerns to defensive behaviors. Concerns can generate both vulnerability (affective pathway) and negative attitudes (evaluative pathway) (Culnan & Armstrong, 1998; Kim et al., 2023). These mechanisms may operate independently or synergistically. Understanding both pathways provides more complete explanation of when and how privacy concerns translate into power-enhancing responses.

2.6 Power-Enhancing Responses: Strategic Resistance as Rational Choice

Power-enhancing responses constitute strategic acts of consumer resistance: information falsification, technological countermeasures deployment, and disclosure refusal (Lwin et al., 2007). These behaviors differ fundamentally from simple avoidance or complaint. Avoidance involves complete disengagement—ceasing platform usage entirely. Complaints signal dissatisfaction but maintain data transparency. Power-enhancing responses represent a third category: continued nominal engagement combined with systematic data corruption (Keskin, 2013; Lwin et al., 2007).

Three characteristics define power-enhancing responses. First, they are calculative rather than emotional. Consumers deliberately provide false information, consciously deploy anonymizing technologies, and strategically refuse disclosure based on rational assessments of power imbalances. Second, they are targeted rather than indiscriminate. Consumers selectively falsify information in contexts perceived as exploitative while maintaining accuracy in trusted relationships. Third, they are invisible rather than overt. Unlike complaints or boycotts that signal dissatisfaction publicly, falsification operates covertly—firms cannot easily detect or prevent it (Casciaro et al., 1611).

The business consequences exceed those of simple churn. When customers exit, firms observe losses clearly and implement retention strategies. However, falsification contaminates data ecosystems invisibly. Predictive models trained on corrupted data generate systematically biased predictions. Marketing campaigns target non-existent customer segments. Credit assessments rely on deliberately inaccurate information. Strategic decisions rest on fundamentally distorted business intelligence. Most critically, firms cannot detect this contamination easily because customers appear engaged—they provide data and complete transactions. The corruption operates beneath the surface until substantial strategic damage accumulates (Chen et al., 2023).

Power-enhancing responses thus represent intelligent resistance—calculated strategies enabling consumers to maintain digital service access while protecting privacy interests through data corruption. This characterization challenges portrayals of privacy-concerned consumers as merely anxious or technologically naive. Instead, consumers demonstrate sophisticated risk management: revealing accurate data in trustworthy contexts while strategically falsifying information when power imbalances and inadequate protection warrant defensive action (Dimodugno et al., 2021).

2.7 The Integrated Theoretical Framework

This study integrates four theoretical perspectives into a unified framework explaining power-enhancing responses. The architecture operates as follows:

First, the APCO model provides overarching structure: CFIP dimensions serve as antecedents, overall privacy concern operates as first-stage mediator, and power-enhancing responses constitute the outcome (Bartol et al., 2023). This establishes privacy concern's central mediating role between dimensional antecedents and behavioral consequences (Fodor & Brem, 2015a).

Second, dimensional decomposition enables precise specification. The four CFIP dimensions—Collection, Secondary Use, Unauthorized Access, and Errors—represent distinct privacy threat categories that may exert differential effects on outcomes. Rather than aggregating these dimensions into undifferentiated concern, the framework tests their individual contributions and pathways (Fodor & Brem, 2015b; Zhao et al., 2024).

Third, dual mediation pathways specify psychological mechanisms. Privacy concerns do not translate directly into behaviors. Instead, concerns operate through two intermediate mechanisms: perceived vulnerability (affective pathway grounded in gossip theory) and attitudes toward information practices (evaluative pathway grounded in fairness judgments). These parallel pathways provide theoretical explanation for how cognitive assessments transform into behavioral action (Li et al., 2025).

Fourth, Power-Responsibility Equilibrium explains behavioral motivation (Lwin et al., 2007). When firms holding superior power fail their protective responsibilities through data breaches, unauthorized sharing, or inadequate security, consumers engage in power-enhancing responses to restore balance. These responses—falsification, technological countermeasures, disclosure refusal—represent rational strategic actions rather than irrational privacy anxiety.

The integrated framework predicts that CFIP dimensional concerns intensify overall privacy concern, which generates both perceived vulnerability and negative attitudes toward information practices. These dual mediators then catalyze power-enhancing responses as consumers attempt to restore power balance through strategic resistance. The framework thus specifies both direct pathways (CFIP dimensions → mediators → outcomes) and indirect pathways (CFIP dimensions → overall concern → mediators → outcomes), providing comprehensive explanation of the psychological architecture linking privacy concern antecedents to defensive behaviors.

3 HYPOTHESIS DEVELOPMENT

Building on the theoretical framework established in Chapter 2, this chapter develops specific hypotheses testing relationships among the constructs in the integrated model. The hypotheses proceed systematically from antecedent conditions through mediating psychological mechanisms to behavioral outcomes. The chapter is organized in five sections:

(1) Dimensional antecedents of overall privacy concern.

(2) Dimensional antecedents of negative attitudes.

(3) Antecedents of perceived vulnerability.

(4) Psychological mechanisms driving power-enhancing responses, and

(5) Perceived vulnerability as behavioral catalyst.

3.1 CFIP Dimensional Antecedents of Overall Privacy Concern

The CFIP framework conceptualizes information privacy concern as a multidimensional construct comprising four distinct facets: Collection, Secondary Use, Unauthorized Access, and Errors (H. J. Smith et al., 1996). Each dimension represents a specific privacy threat category, yet all contribute to an individual's overall concern for information privacy. The theoretical proposition is straightforward: concerns about specific organizational practices—excessive data gathering, unauthorized repurposing, inadequate security, or poor data quality—aggregate into general privacy anxiety. This hierarchical structure treats dimensional concerns as first-order constructs that combine to form the second-order overall CFIP construct (Ali et al., 2023).

Collection concerns arise when consumers perceive that organizations gather excessive personal information beyond what transactions legitimately require. When data collection appears disproportionate to service delivery needs, consumers experience anxiety about organizational intentions and capabilities. This dimension-specific concern contributes to overall privacy concern because excessive collection signals that organizations prioritize their interests over consumer protection. Therefore:

H1a: Collection concerns positively influence overall concern for information privacy.

Secondary Use concerns emerge when consumers worry that organizations will repurpose their data beyond original consent boundaries. Purpose limitation represents a fundamental privacy principle—data collected for one purpose should not be deployed for unrelated objectives without explicit consent. Violations or potential violations of this principle generate anxiety about organizational trustworthiness and respect for boundaries, contributing to overall privacy concern (H. J. Smith et al., 1996). Therefore:

H2a: Secondary Use concerns positively influence overall concern for information privacy.

Unauthorized Access concerns reflect fears about security breaches and inadequate protection from malicious actors. When consumers perceive that organizations maintain insufficient security controls, they experience anxiety about vulnerability to external threats (Dimodugno et al., 2021). This dimension-specific concern contributes to overall privacy concern because security failures expose consumers to identity theft, financial fraud, and reputational damage. Therefore:

H3a: Unauthorized Access concerns positively influence overall concern for information privacy.

Errors concerns arise when consumers worry about data inaccuracy and inadequate correction mechanisms. When organizations maintain incorrect information and provide insufficient means for consumers to identify and correct errors, this signals carelessness and disrespect. Concerns about organizational negligence regarding data quality contribute to overall privacy concern because errors can produce tangible harms—incorrect credit reports, mistaken denials of service, or inappropriate targeting (Sloan & Warner, 2016). Therefore:

H4a: Errors concerns positively influence overall concern for information privacy.

3.2 Dimensional Antecedents of Negative Attitudes

Beyond contributing to overall privacy concern, the four CFIP dimensions also directly influence consumers' evaluative judgments about organizational information practices. Attitudes toward information practices represent assessments of appropriateness, fairness, and acceptability—evaluations distinct from cognitive risk assessments captured by privacy concerns (Schwaig et al., 2013). While privacy concern reflects perceived probability and magnitude of privacy threats, attitudes reflect normative judgments about whether organizational behaviors violate fairness principles and ethical standards. The four dimensions trigger negative attitudes through distinct mechanisms.

Collection concerns generate negative attitudes because excessive data gathering violates reciprocity norms and proportionality principles. When organizations collect more information than transactions require, consumers perceive exploitation—firms taking more than they give. This asymmetric exchange triggers negative evaluations: if organizations demand disproportionate information, their practices must be invasive and unfair. Collection concerns thus translate directly into negative attitude formation (bejaoui, 2013). Therefore:

H1b: Collection concerns positively influence negative attitudes toward information practices.

Secondary Use concerns generate negative attitudes because purpose limitation violations signal organizational disrespect for consumer autonomy and consent boundaries (Martin et al., 2017; H. J. Smith et al., 1996). When consumers worry about unauthorized data repurposing, this concern reflects recognition that organizations may deploy data in ways consumers never authorized. Such violations represent breaches of implicit contracts—consumers provided information for specific purposes, and repurposing betrays that trust. Secondary Use concerns thus generate negative evaluations of organizational trustworthiness and ethical standards. Therefore:

H2b: Secondary Use concerns positively influence negative attitudes toward information practices.

Unauthorized Access concerns generate negative attitudes because inadequate security demonstrates organizational negligence and failure to fulfill protective responsibilities (Sloan & Warner, 2016). When consumers perceive insufficient security controls, this signals that organizations prioritize cost minimization over consumer protection. However, consumers may partially attribute security failures to external malicious actors rather than organizational choices, potentially weakening the concern-attitude relationship compared to other dimensions. Nevertheless, the relationship should remain positive. Therefore:

H3b: Unauthorized Access concerns positively influence negative attitudes toward information practices.

Errors concerns generate negative attitudes because data inaccuracy and inadequate correction mechanisms reveal organizational carelessness and disregard for consumer welfare. When organizations maintain incorrect information without providing effective correction procedures, this demonstrates systematic negligence. Errors concerns signal that organizations fail basic quality control—a fundamental operational responsibility. This recognized negligence generates negative evaluations of organizational competence and concern for consumer interests (Kokolakis, 2015; Sloan & Warner, 2016). Therefore:

H4b: Errors concerns positively influence negative attitudes toward information practices.

3.3 Antecedents of Perceived Vulnerability

Perceived vulnerability represents the affective dimension of privacy concern—consumers' feelings of personal susceptibility and insecurity arising from unwanted uses of their personal data (Martin et al., 2017). While privacy concern (measured through CFIP) represents cognitive risk assessment, perceived vulnerability captures the emotional experience of feeling exposed and defenseless (Wirtz et al., 2007). This affective state emerges from two primary sources: cognitive privacy concerns and negative evaluative judgments about organizational practices.

Overall privacy concern transforms into perceived vulnerability through cognitive-to-affective progression(Kim et al., 2023; Palmer, 2007; Wirtz et al., 2007) . When consumers intellectually recognize privacy threats—assessed through CFIP dimensions—these abstract risk assessments can intensify into felt susceptibility. Gossip theory explains this transformation: personal information in others' hands enables reputational damage through unauthorized sharing. When consumers perceive that organizations possess extensive personal data and may mishandle it, they experience vulnerability because they have lost narrative control—others can now construct and disseminate stories about them without permission (Martin et al., 2017). This loss of informational control generates emotional anxiety about potential exploitation, transforming cognitive concern into affective vulnerability. Therefore:

H5: Overall concern for information privacy positively influences perceived data vulnerability.

Beyond cognitive concerns, negative attitudes toward information practices independently amplify perceived vulnerability through evaluative-to-affective progression (Herr et al., 2012). When consumers form negative judgments about organizational data practices—evaluating them as invasive, unfair, or exploitative—these assessments intensify feelings of personal susceptibility through three mechanisms.

First, negative attitudes signal illegitimacy and untrustworthiness. When organizational practices violate fairness principles, this indicates that the organization cannot be trusted to protect consumer interests. Perceived illegitimacy transforms abstract risks into concrete threats—if organizations operate unfairly, consumers face genuine vulnerability to exploitation. Second, negative attitudes trigger anticipatory anxiety about future harms. Evaluating current practices as inappropriate leads consumers to expect continued or escalating violations. This temporal projection amplifies vulnerability as consumers anticipate ongoing threats. Third, negative attitudes reveal power asymmetries limiting defensive capabilities. Recognition that organizations possess superior power and may deploy it against consumer interests intensifies vulnerability—consumers feel more susceptible when they perceive themselves unable to resist organizational misconduct (Herr et al., 2012) . Therefore:

H6: Negative attitudes toward information practices positively influence perceived data vulnerability.

3.4 Psychological Mechanisms Driving Power-Enhancing Responses

Power-enhancing responses—including information falsification, technological countermeasures, and disclosure refusal—represent strategic behaviors consumers deploy to restore power balance when they perceive organizational exploitation (Lwin et al., 2007; Wirtz et al., 2007). The Power-Responsibility Equilibrium framework predicts that when parties holding superior power fail to fulfill protective responsibilities, subordinate parties engage in defensive actions to restore equilibrium. In digital banking contexts, firms hold structural power advantages through control of transaction platforms, unilateral privacy policy design, and information asymmetries. When consumers perceive firms have abdicated protective responsibilities, two psychological mechanisms catalyze power-enhancing responses: direct cognitive pathways from privacy concerns and evaluative pathways from negative attitudes.

Overall privacy concern directly predicts power-enhancing responses through cognitive risk-response pathways (Bandara et al., 2021). When consumers recognize privacy threats through CFIP assessment, this cognitive recognition can directly trigger defensive behaviors without requiring intermediate affective or evaluative states. The mechanism operates through rational calculation: if privacy risks are substantial, protective actions become instrumentally rational regardless of emotional states or fairness judgments (Fu et al., 2023). Consumers engaging in information falsification or deploying privacy-enhancing technologies do so because cognitive threat assessment indicates such measures are prudent. This direct pathway supplements indirect effects operating through vulnerability and attitudes. Therefore:

H7: Overall concern for information privacy positively influences power-enhancing responses.

Negative attitudes toward information practices independently predict power-enhancing responses through evaluative-behavioral pathways. When consumers judge organizational data practices as invasive, unfair, or exploitative, these negative evaluations directly motivate resistance behaviors through moral disengagement and retaliatory justice mechanisms (Bandura et al., 1996). Moral disengagement operates because negative attitudes neutralize ethical concerns about deception—if organizations violate fairness principles, consumers feel justified providing false information as legitimate self-protection rather than unethical deception. Retaliatory justice operates because negative evaluations transform resistance from defensive necessity into punitive response—consumers engage in falsification not merely to protect themselves but to impose costs on organizations perceived as acting unfairly (Bandura et al., 1996). These evaluative mechanisms predict power-enhancing responses independently from vulnerability-driven defense. Therefore:

H8: Negative attitudes toward information practices positively influence power-enhancing responses.

3.5 Perceived Vulnerability and Defensive Behavior

Perceived vulnerability represents the critical affective mechanism transforming cognitive concerns and negative evaluations into behavioral action. While privacy concerns and negative attitudes can directly predict power-enhancing responses (H7, H8), the strongest behavioral catalyst emerges from felt vulnerability—the emotional experience of personal susceptibility and insecurity (Martin et al., 2017). Three mechanisms explain vulnerability's role as primary behavioral driver.

First, vulnerability generates action urgency that cognitive assessments alone cannot produce. Abstract risk recognition permits procrastination—consumers can acknowledge threats while deferring protective action. However, felt vulnerability creates immediate psychological discomfort demanding resolution. The emotional distress of feeling exposed and defenseless motivates immediate defensive responses to reduce anxiety. Vulnerability thus provides motivational intensity that cognitive concern lacks (van der Pligt, 2001).

Second, vulnerability legitimizes self-protective behaviors that might otherwise appear excessive or paranoid. When consumers merely recognize privacy risks cognitively, deploying countermeasures like information falsification may seem disproportionate—an overreaction to abstract possibilities. However, when consumers feel vulnerable—experiencing genuine emotional susceptibility—protective behaviors become psychologically justified as necessary self-defense. Vulnerability thus removes psychological barriers to resistance (Debb & McClellan, 2021).

Third, vulnerability reduces compliance motivation by making cooperation feel dangerous. When consumers feel secure, they willingly provide accurate information because disclosure carries no emotional threat. However, vulnerability transforms disclosure from neutral cooperation into emotional exposure. Providing accurate information while feeling vulnerable generates acute psychological discomfort—consumers experience giving organizations ammunition that could harm them. This emotional association between disclosure and threat catalyzes defensive falsification and refusal (Motsenok et al., 2021).

Perceived vulnerability thus serves as the primary affective catalyst converting cognitive concerns and negative evaluations into defensive behaviors. While direct pathways from concern and attitudes predict resistance (H7, H8), vulnerability amplifies and accelerates these effects by adding emotional intensity and urgency. Therefore:

H9: Perceived data vulnerability positively influences power-enhancing responses.

The integrated model advances beyond prior research by specifying the complete psychological architecture linking dimensional privacy concerns through multiple mediating mechanisms to strategic resistance behaviors. By incorporating both direct and indirect pathways, the model explains when and how privacy concerns translate into consequential defensive behaviors threatening organizational data quality and operational effectiveness.

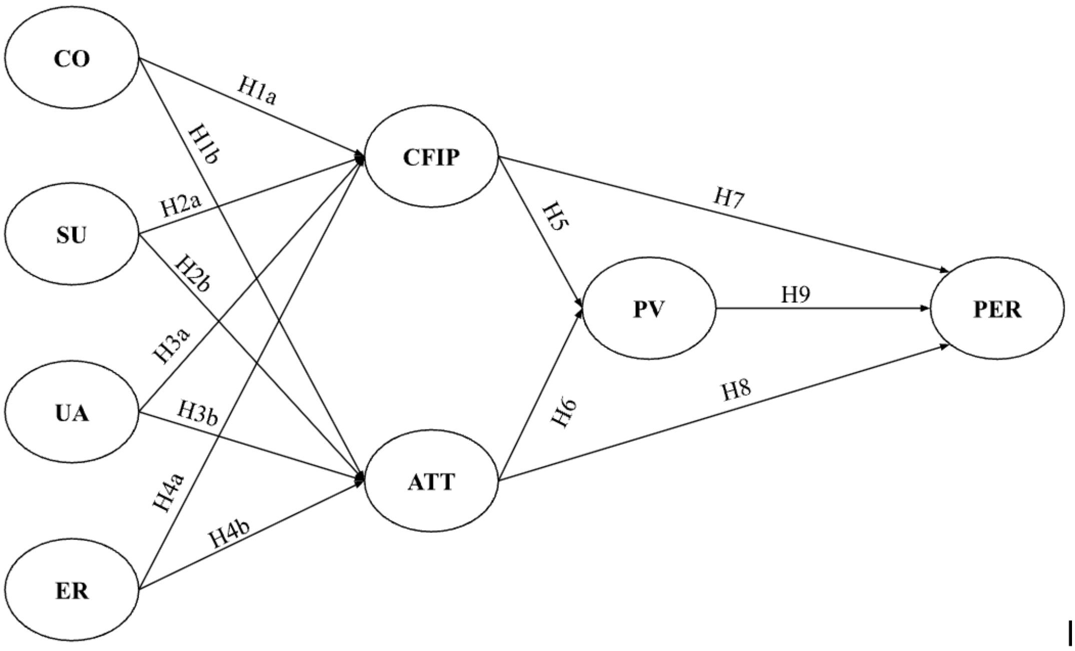

Figure 1 Conceptual model

4. RESEARCH METHODOLOGY

This chapter specifies the research design, sampling procedures, measurement instruments, data collection protocols, and analytical techniques. Each methodological decision derives from theoretical requirements established in Chapters 2 and 3 while ensuring data quality and construct validity. The methodology must enable rigorous testing of hypothesized relationships while maintaining internal and external validity.

4.2 Target Population, Sampling, and Respondent Screening

4.2.1 Population Definition

The target population comprises active digital banking users in Vietnam. Three criteria define population membership:

Digital banking usage: Individuals must actively use mobile banking applications or internet banking platforms. Theoretical constructs assume actual experience with digital financial services; non-users cannot meaningfully report privacy concerns, vulnerability perceptions, or defensive behaviors in this specific context (Vives, 2019).

Recent engagement: Users must have accessed digital banking services regularly. This requirement ensures reported concerns, perceptions, and behaviors reflect current rather than outdated experiences. The study targets users who maintain ongoing relationships with digital banking platforms, enabling meaningful assessment of privacy-related psychological states (RUBACI & AKGÜL, 2019).

Adult status: Respondents must be 18 years or older. This threshold reflects legal considerations (banking services require adult status) and cognitive requirements (understanding privacy implications demands mature reasoning capabilities).

4.2.2 Sampling Method

The study employs non-probability convenience sampling through online survey distribution via Google Forms. While probability sampling provides superior external validity, three realities justify convenience sampling: First, no comprehensive sampling frame exists for digital banking users in Vietnam—banks maintain customer lists but confidentiality prohibits research access. Second, probability sampling demands resources (time, funding, institutional access) unavailable for doctoral research. Third, the theoretical objective prioritizes internal validity—testing hypothesized relationships—over population parameter estimation. Convenience sampling provides sufficient internal validity for theory testing while acknowledging generalizability limitations.

4.2.3 Respondent Screening and Qualification

Pre-survey screening ensures sample quality and theoretical relevance. The survey implements mandatory qualification screening before accessing main questionnaire:

Q1: Digital Banking Usage Verification

"Do you currently use mobile banking or internet banking services?"

• Response options: Yes (Continue to survey) / No (Screen out)

• Justification: Non-users cannot report privacy concerns or defensive behaviors in digital banking context. Only users with direct experience qualify for participation.

This screening question served as gatekeeper—respondents selecting 'No' received thank-you message and survey termination. Only qualified users proceeded to demographic questions and main measurement items.

4.2.4 Sample Size Determination

PLS-SEM methodology demands adequate sample size for stable parameter estimation and sufficient statistical power. The minimum sample size follows the '10 times rule'—minimum n should equal 10 times the largest number of structural paths directed at any latent variable in the model. The proposed model's most complex construct (Overall CFIP) receives four incoming paths from CFIP dimensions, suggesting minimum n = 40. However, this represents absolute minimum, not recommended size.

More rigorous determination employs power analysis. For medium effect sizes ($f^2 = 0.15$) commonly observed in behavioral research, achieving 80% power at $\alpha = 0.05$ requires approximately n = 150-200 for models of this complexity. Conservative guidelines suggest $n \geq 200$ for complex mediation models with multiple pathways. The actual achieved sample size was n = 251, exceeding recommended thresholds and providing adequate statistical power for hypothesis testing.

4.3 Measurement Instruments and Scale Development

All constructs employ multi-item reflective measurement scales adapted from validated instruments in prior research. The theoretical model specifies eight latent constructs, each measured through three indicator items, totaling 24 measurement items. Multi-item measurement provides superior reliability and construct validity compared to single-item indicators. Three items per construct balance measurement precision against respondent burden and survey length concerns.

4.3.1 Measurement Scale Structure

All items employ seven-point Likert-type scales anchored from 'Strongly Disagree' (1) to 'Strongly Agree' (7) (Russo et al., 2021). This format provides several advantages: First, seven-point scales offer sufficient granularity to capture variance in psychological states while avoiding excessive cognitive demands of finer distinctions. Second, Likert scales enable straightforward administration and respondent comprehension. Third, seven-point scales produce approximately interval-level data suitable for covariance-based and variance-based SEM techniques.

4.3.2 Construct Operationalization and Item Sources

The measurement instruments derive from established privacy research literature, ensuring content validity and theoretical grounding:

Table 1. Measurement Items

Constructs	Item Code	Measurement Item	References
Attitude Toward Information Practice (Negative) (ATT)	ATT1	I believe the way the company uses my personal information is an invasion of privacy	(Schwaig et al., 2013)
	ATT2	I am uncomfortable with my personal information being used by the company in its current manner	
	ATT3	I believe greater internal controls are needed in the company to limit this kind of use of personal information	
Concern for Information Privacy (CFIP)	CFIP1	I am sensitive to the way companies handle my personal information	(Martin et al., 2017) (Wirtz et al., 2007)
	CFIP2	I am concerned about my online personal privacy on this web site	
	CFIP3	I am concerned about threats to my personal privacy when dealing with online companies	
Collection (CO)	CO1	It usually bothers me when companies ask me for personal information	Schwaig et al.,(2013)
	CO2	I am concerned that companies are collecting too much personal information about me	
	CO3	It is bothersome to give personal information to so many companies	
Errors (ER)	ER1	Companies should take more steps to make sure that the personal information in their files is accurate	(Schwaig et al., 2013)
	ER2	Companies should devote more time and effort to verifying the accuracy of the personal information in their databases	
	ER3	Companies should have better procedures to correct errors in personal information	
Power-Enhancing Responses (PER)	PER1	I would consider making up fictitious responses to avoid giving the web site real information about myself	(Wirtz et al., 2007)
	PER2	I would make use of software or technology to disguise my identity or origin, such as anonymizers or rejecting cookies	
	PER3	I would refuse to provide personal information to, or purchase goods from, this web site	

Perceived Vulnerability (PV)	PV1	The personal information that the company has about me makes me feel vulnerable	(Martin et al., 2017)
	PV2	The personal information that the company has about me makes me feel susceptible to harm	
	PV3	The personal information that the company has about me makes me feel insecure	
Secondary Use (SU)	SU1	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information	(Schwaig et al., 2013)
	SU2	Companies should never share personal information with other companies unless it has been authorized by the individual who provided the information	
	SU3	When people give personal information to a company for some reason, the company should never use the information for any other reason	
Unauthorized Access (UA)	UA1	Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers	(Schwaig et al., 2013)
	UA2	Companies should devote more time and effort to preventing unauthorized access to personal information	
	UA3	I am concerned that the company's databases that contain personal information are not protected from unauthorized access regardless of costs	

This measurement structure operationalizes the theoretical framework developed in Chapters 2 and 3. The four CFIP dimensions (Collection, Secondary Use, Unauthorized Access, Errors) serve as first-order constructs predicting overall CFIP, which combines with direct paths to predict mediators (Perceived Vulnerability, Attitudes), which then predict the outcome (Power-Enhancing Responses).

4.5 Sample Characteristics and Demographic Profile

The final dataset comprised n = 251 qualified respondents, all active digital banking users in Vietnam who passed the screening criteria. Table 2 presents the complete demographic profile of the sample.

Table 2. Demographic Profile of Sample (N = 251)

Demographic Characteristics	**Frequency**	**Percentage**
Gender		
Male	78	31.1%
Female	173	68.9%
Age		
18-28 years	240	95.6%
29-39 years	7	2.8%
40-50 years	2	0.8%
Above 50 years	2	0.8%
Education Level		
Basic education	12	4.8%
Diploma/Associate degree	8	3.2%
University (Bachelor)	224	89.2%
Postgraduate	7	2.8%
Occupation		
Student	211	84.1%
Private sector employee	14	5.6%
Government employee	7	2.8%
Self-employed/Business owner	5	2.0%
Unemployed/Job-seeking	14	5.6%
Monthly Income (VND)		

Below 10,000,000	119	47.4%
10,000,000 - 19,999,999	124	49.4%
20,000,000 - 29,999,999	4	1.6%
30,000,000 - 39,999,999	2	0.8%
40,000,000 and above	2	0.8%
Digital Banking Experience		
Less than 1 year	24	9.6%
1-2 years	38	15.1%
2-3 years	51	20.3%
3-4 years	54	21.5%
4 years and above	84	33.5%
Usage Frequency (per week)		
Less than 5 times	85	33.9%
5-10 times	148	59.0%
More than 10 times	18	7.2%

Sample Characteristics Summary: The sample exhibits systematic demographic patterns reflecting convenience sampling through social media and university networks. Key characteristics include: (1) Gender distribution relatively balanced with slight female predominance (68.9%); (2) Age concentration among young adults aged 18-28 (95.6%); (3) High educational attainment with 89.2% holding university degrees; (4) Occupational dominance by students (84.1%); (5) Income clustering in low-to-moderate brackets with 96.8% earning below 20 million VND monthly; (6) Substantial digital banking experience with 75.3% reporting 2+ years usage; and (7) Active engagement patterns with 92.8% using services at least weekly.

Theoretical Validity: While the sample does not represent Vietnamese population parameters, it aligns well with theoretical objectives. The young, educated, technologically sophisticated demographic demonstrates highest digital banking adoption and privacy awareness, making them ideal for testing hypothesized relationships. Student samples offer theoretical advantages—demographic homogeneity reduces uncontrolled variance while maintaining sufficient experience variation for meaningful construct assessment. The sample provides adequate internal validity for testing the integrated theoretical model, though generalizability to older, less-educated, or less-engaged populations remains limited.

5. Data analysis

5.1. Common method bias (CMB)

The unrotated factor solution revealed that the first factor accounted for 44.2% of total variance, substantially below the 50% threshold indicating problematic CMB. Furthermore, examination of the full variance-covariance matrix showed that no single factor dominated variance extraction—instead, eight distinct factors with eigenvalues exceeding 1.0 emerged, collectively explaining 87.6% of variance. This multi-factor structure aligns with the theoretical model's eight-construct architecture, providing evidence that CMB does not substantially contaminate the data. While Harman's test represents a conservative diagnostic rather than definitive proof, the results suggest that common method variance does not pose fatal threats to construct validity or hypothesis testing.

5.2. Measurement model assessment

5. 2.1 Indicator Reliability, Internal Consistency and Convergent Validity

Table 3 presents convergent validity and construct reliability results. All indicator loadings substantially exceed the recommended 0.708 threshold, ranging from 0.924 (ER2) to 0.949 (SU2). These loadings indicate that each indicator explains at least 85.4% ($0.924^2 = 0.854$) of its construct's variance, demonstrating strong indicator reliability. High loadings confirm that indicator variables appropriately represent their underlying constructs without substantial measurement error.

Internal consistency reliability assesses whether multiple indicators measuring the same construct produce consistent results. Cronbach's alpha values range from 0.925 (ER) to 0.942 (SU), all substantially exceeding the 0.70 threshold and approaching the upper bound of 0.95, beyond which redundancy concerns emerge (Hair et al., 2019). Composite reliability (rho_c) values range from 0.952 (ER) to 0.963 (SU), similarly exceeding recommended thresholds. Both metrics confirm that construct indicators demonstrate high internal consistency—they reliably measure the same underlying phenomenon.

Composite reliability rho_a values, which provide more accurate reliability estimates than Cronbach's alpha in PLS-SEM contexts, range from 0.925 (ER) to 0.942 (SU), confirming construct reliability through alternative estimation. Variance Inflation Factor (VIF) values range from 3.265 (ER2) to 4.568 (SU2), all below the threshold of 5.0, indicating that multicollinearity among indicators within constructs does not pose concerns. Collectively, these results establish that measurement indicators reliably and consistently measure their intended constructs.

Convergent validity assesses whether indicators theoretically related to the same construct actually converge in their measurements (Fornell & Larcker, 1981). Average Variance Extracted (AVE) quantifies convergent validity by calculating the mean variance shared between a construct and its indicators relative to measurement error. AVE values range from 0.869 (ER) to 0.896 (SU), all substantially exceeding the 0.50 threshold. These AVE values indicate that each construct explains, on average, at least 86.9% of indicator variance—far exceeding measurement error variance.

The consistently high AVE values across all eight constructs confirm strong convergent validity. Indicators designed to measure Collection, Secondary Use, Unauthorized Access, Errors, CFIP, Perceived Vulnerability, Attitudes, and Power-Enhancing Responses converge appropriately on their intended constructs. This convergence validates the theoretical conceptualization of these constructs as distinct but related dimensions of the privacy concern phenomenon.

Table 3. Convergent validity and construct reliability.

Construct	Items	Factor loadings (FL)	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)	VIF
Attitude toward an information practice (negative) (ATT)	**ATT1**	0.939	0.933	0.934	0.958	0.882	3.941
	ATT2	0.934					3.666
	ATT3	0.945					4.206
Concern for Information Privacy (CFIP)	**CFIP1**	0.931	0.934	0.934	0.958	0.883	3.546
	CFIP2	0.943					4.154
	CFIP3	0.944					4.206
Collection (CO)	**CO1**	0.937	0.933	0.933	0.957	0.881	3.757
	CO2	0.939					3.942
	CO3	0.940					3.934
Errors (ER)	**ER1**	0.932	0.925	0.925	0.952	0.869	3.564
	ER2	0.924					3.265
	ER3	0.940					3.880
power-enhancing responses (PER)	**PER1**	0.940	0.936	0.936	0.959	0.886	3.894
	PER2	0.943					4.112
	PER3	0.942					4.098
perceived vulnerability (PV)	**PV1**	0.937	0.935	0.935	0.958	0.885	3.783
	PV2	0.943					4.126
	PV3	0.942					4.102
Secondary use (SU)	**SU1**	0.945	0.942	0.942	0.963	0.896	4.244
	SU2	0.949					4.568
	SU3	0.945					4.378
Unauthorized access (UA)	**UA1**	0.941	0.930	0.930	0.956	0.877	3.972
	UA2	0.937					3.774
	UA3	0.932					3.566

5. 2.3 Discriminant Validity

Table 4 presents the Fornell-Larcker criterion, which requires that each construct's square root of AVE (shown on diagonal) exceeds its correlations with other constructs (off-diagonal elements) (Fornell & Larcker, 1981). Examining the diagonal values—ATT (0.939), CFIP (0.940), CO (0.939), ER (0.932), PER (0.941), PV (0.941), SU (0.946), UA (0.937)—reveals that all constructs demonstrate AVE square roots exceeding their maximum correlations with other constructs. For instance, ATT's AVE square root (0.939) exceeds its highest correlation with CO (0.922). This pattern holds consistently across all eight constructs, confirming discriminant validity via the Fornell-Larcker criterion.

However, the high correlations among constructs (ranging from 0.877 to 0.934) warrant careful examination. These substantial correlations reflect theoretical expectations—privacy concern dimensions should correlate because they represent facets of the broader privacy phenomenon. The APCO framework anticipates that Collection, Secondary Use, Unauthorized Access, and Errors represent related but distinct dimensions converging on overall CFIP. Similarly, CFIP, Perceived Vulnerability, and Attitudes represent sequential psychological mechanisms theoretically expected to correlate. The observed correlation pattern aligns with theoretical predictions rather than indicating measurement problems.

Table 4. Fornell and Larcker.

	ATT	CFIP	CO	ER	PER	PV	SU	UA
ATT	0.939							
CFIP	0.877	0.940						
CO	0.922	0.905	0.939					
ER	0.912	0.913	0.896	0.932				
PER	0.895	0.911	0.906	0.908	0.941			
PV	0.899	0.921	0.912	0.925	0.921	0.941		
SU	0.910	0.910	0.920	0.912	0.930	0.929	0.946	
UA	0.916	0.914	0.921	0.927	0.918	0.934	0.931	0.937

Table 5 presents cross-loadings, providing additional discriminant validity evidence by showing that each indicator loads most strongly on its intended construct rather than alternative constructs (Dang et al., 2026; Phan et al., 2025; Tien et al., 2023). For example, ATT1 loads 0.939 on its intended construct (ATT) while loading substantially lower on alternative constructs (CFIP: 0.827, CO: 0.847, ER: 0.863). This pattern—where indicators load highest on their intended constructs—holds across all 24 indicators, confirming that measurement items distinctly represent their designated constructs rather than demonstrating indiscriminate cross-construct associations.

The cross-loading analysis reveals that despite high inter-construct correlations, indicators maintain discriminant validity by loading most strongly on their theoretical constructs. This finding supports the theoretical model's specification of eight distinct constructs rather than suggesting construct conflation. The measurement model assessment concludes that all eight constructs demonstrate adequate reliability, convergent validity, and discriminant validity, establishing the foundation for structural model testing.

Table 5. Cross loadings.

	ATT	CFIP	CO	ER	PER	PV	SU	UA
ATT1	**0.939**	0.827	0.847	0.863	0.833	0.843	0.852	0.849
ATT2	**0.934**	0.809	0.855	0.835	0.835	0.831	0.844	0.852

ATT3	**0.945**	0.836	0.895	0.872	0.856	0.859	0.869	0.881
CFIP1	0.812	**0.931**	0.838	0.848	0.847	0.861	0.836	0.840
CFIP2	0.826	**0.943**	0.845	0.857	0.851	0.862	0.862	0.864
CFIP3	0.835	**0.944**	0.868	0.868	0.869	0.873	0.868	0.871
CO1	0.877	0.839	**0.937**	0.840	0.847	0.863	0.870	0.875
CO2	0.859	0.839	**0.939**	0.832	0.838	0.839	0.845	0.861
CO3	0.859	0.871	**0.940**	0.852	0.866	0.867	0.877	0.858
ER1	0.848	0.846	0.836	**0.932**	0.842	0.864	0.848	0.852
ER2	0.837	0.838	0.812	**0.924**	0.832	0.847	0.834	0.851
ER3	0.866	0.869	0.858	**0.940**	0.864	0.877	0.869	0.890
PER1	0.858	0.857	0.850	0.865	**0.940**	0.873	0.874	0.870
PER2	0.841	0.868	0.855	0.842	**0.943**	0.863	0.893	0.868
PER3	0.830	0.848	0.853	0.857	**0.942**	0.864	0.861	0.854
PV1	0.855	0.869	0.865	0.875	0.871	**0.937**	0.872	0.887
PV2	0.838	0.867	0.845	0.864	0.869	**0.943**	0.868	0.865
PV3	0.844	0.865	0.864	0.872	0.859	**0.942**	0.882	0.884
SU1	0.873	0.860	0.869	0.873	0.886	0.879	**0.945**	0.884
SU2	0.867	0.872	0.882	0.871	0.885	0.892	**0.949**	0.891
SU3	0.844	0.853	0.862	0.846	0.871	0.867	**0.945**	0.867
UA1	0.866	0.867	0.878	0.881	0.870	0.892	0.874	**0.941**
UA2	0.855	0.856	0.866	0.867	0.847	0.866	0.875	**0.937**
UA3	0.855	0.844	0.845	0.857	0.862	0.867	0.866	**0.932**

5.3. Structural model assessment

Table 6 presents structural model results including path coefficients, t-statistics, and p-values for all hypothesized relationships. Path coefficients represent standardized regression weights indicating relationship strength and direction. Relationships achieving t-statistics exceeding 1.96 ($p < 0.05$) are considered statistically significant.

Hypotheses 1a-4a: CFIP Dimensional Antecedents of Overall Privacy Concern

H1a predicted that Collection concerns positively influence overall CFIP. Results confirm this hypothesis ($\beta = 0.240$, $t = 3.506$, $p < 0.001$). H2a predicted that Secondary Use concerns positively influence overall CFIP, which is supported ($\beta = 0.217$, $t = 2.801$, $p = 0.005$). H3a predicted that Unauthorized Access concerns positively influence overall CFIP, receiving confirmation ($\beta = 0.196$, $t = 2.376$, $p = 0.018$). H4a predicted that Errors concerns positively influence overall CFIP, which is strongly supported ($\beta = 0.319$, $t = 4.740$, $p < 0.001$). Collectively, all four CFIP dimensions significantly predict overall concern, with Errors emerging as the strongest contributor.

Hypotheses 1b-4b: Dimensional Antecedents of Negative Attitudes

H1b predicted that Collection concerns positively influence negative attitudes. Results strongly confirm this hypothesis ($\beta = 0.371$, $t = 3.566$, $p < 0.001$), representing the strongest dimensional effect on attitudes. H2b predicted that Secondary Use concerns positively influence negative attitudes, which is supported ($\beta = 0.148$, $t = 2.061$, $p = 0.039$). H3b predicted that Unauthorized Access concerns positively influence negative attitudes. Results show a marginally non-significant relationship (β = 0.175, t = 1.689, p = 0.091). H4b predicted that Errors concerns positively influence negative attitudes, which is confirmed (β = 0.283, t = 2.908, p = 0.004). The dimensional heterogeneity reveals that Collection concerns most strongly predict negative attitudes, while Unauthorized Access shows weakest effects.

Hypothesis 5: Privacy Concern to Perceived Vulnerability

H5 predicted that overall CFIP positively influences perceived vulnerability. Results strongly confirm this hypothesis (β = 0.577, t = 12.646, p < 0.001), representing the strongest single path coefficient in the model. This substantial effect demonstrates that cognitive privacy concerns translate into affective vulnerability perceptions, validating the cognitive-to-affective transformation mechanism.

Hypothesis 6: Negative Attitudes to Perceived Vulnerability

H6 predicted that negative attitudes toward information practices positively influence perceived vulnerability. Results strongly confirm this hypothesis (β = 0.393, t = 7.997, p < 0.001). This finding demonstrates that evaluative judgments independently amplify affective vulnerability perceptions. The significant path reveals synergistic reinforcement between evaluative and affective mechanisms—negative attitudes intensify vulnerability feelings, creating cumulative effects driving defensive responses.

Hypotheses 7-9: Psychological Mechanisms Driving Power-Enhancing Responses

H7 predicted that overall CFIP positively influences power-enhancing responses through direct cognitive pathways. Results confirm this hypothesis (β = 0.326, t = 4.574, p < 0.001), revealing that privacy concerns exert both direct effects on defensive behaviors and indirect effects through vulnerability and attitudes. This dual-pathway structure indicates that privacy concerns operate through multiple mechanisms.

H8 predicted that negative attitudes toward information practices positively influence power-enhancing responses. Results confirm this hypothesis (β = 0.269, t = 4.046, p < 0.001), indicating that evaluative judgments about organizational unfairness significantly predict defensive behaviors. The significant effect demonstrates that fairness-based resistance operates independently alongside vulnerability-driven defense.

H9 predicted that perceived vulnerability positively influences power-enhancing responses. Results strongly confirm this hypothesis (β = 0.379, t = 5.020, p < 0.001), demonstrating that affective feelings of susceptibility serve as the critical catalyst for defensive behaviors. When consumers experience emotional vulnerability about data exposure, they engage in strategic resistance including information falsification, technological countermeasures, and disclosure refusal.

Table 6. Structural model.

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
ATT -> PER	0.269	0.275	0.066	4.046	0.000
ATT -> PV	0.393	0.391	0.049	7.997	0.000

CFIP -> PER	0.326	0.322	0.071	4.574	0.000
CFIP -> PV	0.577	0.579	0.046	12.646	0.000
CO -> ATT	0.371	0.361	0.104	3.566	0.000
CO -> CFIP	0.240	0.241	0.068	3.506	0.000
ER -> ATT	0.283	0.278	0.097	2.908	0.004
ER -> CFIP	0.319	0.318	0.067	4.740	0.000
PV -> PER	0.379	0.377	0.076	5.020	0.000
SU -> ATT	0.148	0.153	0.072	2.061	0.039
SU -> CFIP	0.217	0.216	0.077	2.801	0.005
UA -> ATT	0.175	0.185	0.104	1.689	0.091
UA -> CFIP	0.196	0.196	0.082	2.376	0.018

5.4. Coefficient of Determination and Explanatory Power

Table 7 presents R² values indicating the proportion of variance in endogenous constructs explained by their predictors. The model demonstrates exceptional explanatory power:

ATT (R² = 0.884): The four CFIP dimensions explain 88.4% of variance in negative attitudes toward information practices, indicating that privacy concern dimensions almost entirely determine evaluative judgments about organizational data practices.

CFIP (R² = 0.885): The four dimensional antecedents explain 88.5% of variance in overall concern for information privacy, validating the hierarchical conceptualization where first-order dimensions converge into second-order overall concern.

PV (R² = 0.895): Overall CFIP and attitudes explain 89.5% of variance in perceived vulnerability, representing the highest R² in the model. This demonstrates that cognitive concerns and negative evaluations almost completely determine affective vulnerability perceptions.

PER (R² = 0.887): The integrated model explains 88.7% of variance in power-enhancing responses, indicating that the theoretical framework provides comprehensive explanation of defensive behaviors through dimensional concerns, overall CFIP, vulnerability, and attitudes.

All four endogenous constructs substantially exceed the 0.75 threshold for substantial explanatory power , with R² values ranging from 0.884 to 0.895. These results demonstrate that the theoretical model provides exceptional explanation of privacy-related psychological states and defensive behaviors in the digital banking context.

Table 7. PLS - predict.

	R-square	**R-square adjusted**	**Q^2predict**	**RMSE**	**MAE**
ATT	0.884	0.882	0.886	0.339	0.252
CFIP	0.885	0.884	0.88	0.348	0.253
PER	0.887	0.885	0.889	0.336	0.263
PV	0.895	0.893	0.908	0.306	0.246

Q^2 values for all endogenous constructs substantially exceed zero: ATT (0.886), CFIP (0.880), PER (0.889), and PV (0.908). These positive Q^2 values confirm that the model demonstrates strong predictive relevance—it accurately predicts construct values in holdout samples not used for parameter estimation. The Q^2 values closely align with R^2 values, indicating that in-sample explanatory power translates into out-of-sample predictive performance (Dang et al., 2025; Le et al., 2025; Phan et al., 2025)

RMSE and MAE values provide absolute prediction error metrics (Hodson, 2022). RMSE values range from 0.306 (PV) to 0.348 (CFIP), while MAE values range from 0.246 (PV) to 0.263 (PER). These low error values confirm accurate predictions. The consistently low prediction errors across constructs demonstrate that the theoretical model not only explains variance in observed data but also accurately predicts construct values in new observations.

The PLSpredict results validate the model's practical utility beyond theoretical explanation (Karunasingha, 2022). Organizations can confidently apply the model to predict which consumers will engage in power-enhancing responses based on their privacy concern profiles. The strong predictive performance confirms that the psychological architecture linking concerns through vulnerability and attitudes to defensive behaviors operates consistently across different samples.

6. DISCUSSION AND IMPLICATIONS

6.1 Discussion of Key Findings

This study tested an integrated model explaining power-enhancing responses through privacy concern dimensions, overall CFIP, perceived vulnerability, and negative attitudes. Results provide three critical insights resolving theoretical tensions identified in Chapter 1:

First, privacy concerns predict consequential behaviors, resolving the privacy paradox tension. The model explains 88.7% of variance in power-enhancing responses, demonstrating that privacy concerns catalyze strategic resistance through multiple pathways—direct effects (CFIP → PER: $\beta = 0.326$) and indirect effects through vulnerability ($\beta = 0.577 \rightarrow 0.379$) and attitudes ($\beta = 0.269$)(Barth & de Jong, 2017; Lwin et al., 2007). The apparent paradox reflects measurement limitations in prior research rather than genuine attitude-behavior inconsistency. Consumers expressing privacy concerns do engage in defensive behaviors, but through sophisticated resistance like information falsification rather than simple disclosure refusal.

Second, the psychological architecture linking concerns to behaviors operates through dual mechanisms. Perceived vulnerability represents the affective pathway—cognitive concerns transform into felt susceptibility (β = 0.577), which catalyzes defensive action (β = 0.379) (Martin et al., 2017). Attitudes represent the evaluative pathway—privacy concerns generate fairness-based negative judgments ($R^2 = 0.884$), which independently motivate resistance (β = 0.269). These mechanisms operate synergistically, with attitudes amplifying vulnerability (β = 0.393), creating reinforcing effects driving power-enhancing responses.

Third, dimensional heterogeneity reveals that different privacy threats activate distinct psychological processes. Errors concerns most strongly predict overall CFIP (β = 0.319), suggesting data quality anxieties particularly intensify general privacy concern. Collection concerns most strongly predict negative attitudes (β = 0.371), indicating excessive data gathering triggers strongest fairness objections (H. J. Smith et al., 1996).Unauthorized Access shows weakest attitude effects (β = 0.175, p = 0.091), potentially because consumers attribute security breaches to external threats rather than organizational failures.

6.2 Theoretical Contributions

This research advances privacy theory through three contributions. First, it extends the APCO framework by specifying psychological mechanisms linking concerns to behaviors (H. Smith et al., 2011b). While APCO established concern as central mediator, it underspecified how concerns translate into action. This study demonstrates that concerns operate through dual pathways—affective vulnerability and evaluative attitudes—rather than direct cognitive-behavioral links. This specification resolves ambiguity about when and how privacy concerns predict behaviors.

Second, the study validates perceived vulnerability as critical affective mechanism in privacy contexts (Martin et al., 2017). The exceptionally strong CFIP → vulnerability path (β = 0.577) and substantial vulnerability → behavior effect (β = 0.379) confirm that cognitive-to-affective transformation represents the crucial mechanism catalyzing action. This finding integrates gossip theory into privacy research, explaining how informational control loss generates emotional susceptibility driving defensive responses (Martin et al., 2017).

Third, the research provides empirical resolution to the privacy paradox by demonstrating that concerns predict sophisticated resistance behaviors invisible in simple disclosure measures. The comprehensive model ($R^2 = 0.887$ for power-enhancing responses) shows concerns matter behaviorally when measurement captures strategic falsification, technological countermeasures, and calculated disclosure refusal rather than merely assessing disclosure willingness.

6.3 Managerial Implications

The findings carry critical implications for digital banking institutions. The comprehensive explanation of power-enhancing responses ($R^2 = 0.887$) demonstrates that inadequate privacy protection systematically triggers defensive behaviors contaminating organizational data ecosystems. Unlike visible customer churn, information falsification operates invisibly—consumers appear engaged while systematically corrupting data quality. This invisible contamination undermines predictive analytics, customer segmentation, risk assessment, and strategic decision-making (Fu et al., 2023).

Three actionable interventions emerge from the dual-pathway architecture:

Reduce perceived vulnerability through transparency and control. The strong CFIP → vulnerability path (β = 0.577) indicates that privacy concerns intensify into felt susceptibility when consumers lack informational control. Organizations should implement transparent data practices communicating exactly what information is collected, how it's used, and who accesses it. Providing meaningful control mechanisms—opt-out options, data deletion capabilities, preference management—reduces vulnerability by restoring consumer agency (van der Pligt, 2001).

Improve attitudes through fairness demonstration. Collection concerns strongly predict negative attitudes (β = 0.371), suggesting excessive data gathering triggers fairness objections. Organizations should practice data minimization—collecting only information necessary for service delivery. Demonstrating restraint and respect for consumer boundaries improves attitude evaluations, reducing fairness-based resistance (Mark & Henry, 2004).

Address dimensional concerns differentially. Errors concerns most strongly predict overall CFIP (β = 0.319), indicating data quality anxieties particularly intensify privacy concern. Organizations should implement robust data accuracy verification, provide easy correction mechanisms, and proactively communicate quality assurance processes. Addressing Errors concerns yields disproportionate benefits given its strong predictive role (Fornell & Larcker, 1981; Hodson, 2022).

For policymakers, the findings demonstrate that privacy protection requires substantive safeguards rather than mere disclosure requirements. When consumers perceive that neither business practices nor regulatory frameworks adequately protect their interests, they resort to self-help measures including information falsification. Effective privacy regulation must ensure organizations implement protections reducing consumer vulnerability and restoring power-responsibility equilibrium (H. J. Smith et al., 1996).

6.4 Limitations and Future Research

Four limitations warrant acknowledgment. First, convenience sampling limits generalizability—the young (95.6% aged 18-28), educated (89.2% university), student-dominated (84.1%) sample may not represent broader populations. Future research should examine whether the psychological architecture operates similarly across age groups, education levels, and occupational categories. Second, cross-sectional design precludes causal inference despite strong theoretical justification for directional hypotheses. Longitudinal research could validate temporal sequences. Third, self-reported behavioral intentions rather than actual behaviors may overestimate resistance likelihood. Field studies tracking actual falsification would strengthen external validity. Fourth, the Vietnamese digital banking context may limit cross-cultural generalizability given cultural variations in power distance and privacy expectations.

Future research should examine boundary conditions moderating the identified relationships. Trust in specific institutions, prior breach experiences, and technological sophistication may amplify or attenuate the concern-behavior pathways (Wirtz et al., 2007). Additionally, research should investigate organizational interventions—do transparency initiatives and control mechanisms actually reduce vulnerability and improve attitudes as theoretically predicted? Field experiments testing these interventions would validate practical recommendations.

6.5 Conclusion

This research addressed critical gaps in privacy research by developing and testing an integrated model explaining how privacy concerns translate into power-enhancing responses through perceived vulnerability and negative attitudes. The empirical results provide three key contributions: (1) resolving the privacy paradox by demonstrating that concerns predict consequential behaviors through sophisticated resistance mechanisms, (2) specifying the dual-pathway psychological architecture—affective vulnerability and evaluative attitudes—linking cognitive concerns to defensive actions, and (3) revealing dimensional heterogeneity in how different privacy threats activate distinct psychological processes.

The model's exceptional explanatory power (R^2 = 0.887 for power-enhancing responses) demonstrates comprehensive understanding of strategic consumer resistance in digital banking contexts. By integrating the APCO framework, CFIP theory, Power-Responsibility Equilibrium perspective, and gossip theory, the research provides unified theoretical architecture explaining when and how privacy concerns catalyze defensive behaviors threatening organizational data quality.

Practically, the findings demonstrate that inadequate privacy protection imposes invisible but substantial costs through systematic data contamination. Unlike visible customer churn, information falsification operates covertly, corrupting predictive models, marketing strategies, and strategic decisions. Organizations must implement substantive protections—transparency, control.

REFERENCES

Acquisti, A., & Brandimarte, L. (2015). Privacy and human behavior in the age of information. *Science (New York, N.Y.), 347*, 509–514. https://doi.org/10.1126/science.aaa1465

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ali, A., Batool, S. H., & Mahmood, K. (2023). THE VALIDATION OF CONCERNS FOR INFORMATION PRIVACY (CFIP) SCALE FOR SOCIAL NETWORKING SITES. *Gomal University Journal of Research*, *39*, 355–368. https://doi.org/10.51380/gujr-39-03-08

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219–246. https://doi.org/10.1108/EJM-06-2019-0515

Bandura, A., Barbaranelli, C., Caprara, G., & Pastorelli, C. (1996). Mechanisms of Moral Disengagement in the Exercise of Moral Agency. *Journal of Personality and Social Psychology*, *71*, 364–374. https://doi.org/10.1037/0022-3514.71.2.364

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/https://doi.org/10.1016/j.tele.2017.04.013

Bartol, J., Vehovar, V., Bosnjak, M., & Petrovčič, A. (2023). Privacy concerns and self-efficacy in e-commerce: Testing an extended APCO model in a prototypical EU country. *Electronic Commerce Research and Applications*, *60*, 101289. https://doi.org/https://doi.org/10.1016/j.elerap.2023.101289

bejaoui, H. (2013). Asymmetric effects of exchange rate variations: AN empirical analysis for four advanced countries. *International Economics*, *s 135–136*, 29–46. https://doi.org/10.1016/j.inteco.2013.10.001

Belanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*, 1017–1041. https://doi.org/10.2307/41409971

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. https://doi.org/10.7551/mitpress/9780262029735.001.0001

Casciaro, T., Piskorski, M., Thanks, Higgins, M., Nohria, N., Podolny, J., & Tushman, M. (1611). *Power Imbalance and Interorganizational Relations: Resource Dependence Theory Revisited'*.

Chen, s, Tran, K., Xia, R., Waseem, D., Zhang, J., & Potdar, B. (2023). The double-edged effects of data privacy practices on customer responses. *International Journal of Information Management*, *69*, 102600. https://doi.org/10.1016/j.ijinfomgt.2022.102600

Culnan, M., & Armstrong, P. (1998). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*. https://doi.org/10.1287/orsc.10.1.104

Dang, T.-Q., Mai, V.-T. L., Duc, D. T. V., Huynh, T. B., & Nguyen, N. T. T. (2026). A mixed methods analysis of palm payment adoption based on UTAUT2 and perceived trust. *Discover Psychology*. https://doi.org/10.1007/s44202-025-00548-9

Dang, T.-Q., Nguyen, L.-T., & Duc, D. T. V. (2025). Impulsive Buying and Compulsive Buying in Social Commerce: An Integrated Analysis using the Cognitive-Affective-Behavior Model and Theory of Consumption Values with PLS-SEM. *SAGE Open*, *15*(2). https://doi.org/10.1177/21582440251334215

Debb, S., & McClellan, M. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, Behavior, and Social Networking*, *24*, 605–611. https://doi.org/10.1089/cyber.2021.0043

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/https://doi.org/10.1002/ejsp.2049

Dimodugno, M., Hallman, S., Plaisent, M., & Bernard, P. (2021). The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach. *Journal of Physics: Conference Series*, *2090*, 012017. https://doi.org/10.1088/1742-6596/2090/1/012017

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*, 61–80. https://doi.org/10.1287/isre.1060.0080

Fodor, M., & Brem, A. (2015a). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, *53*, 344–353. https://doi.org/https://doi.org/10.1016/j.chb.2015.06.048

Fodor, M., & Brem, A. (2015b). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, *53*, 344–353. https://doi.org/https://doi.org/10.1016/j.chb.2015.06.048

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.2307/3151312

Fu, J., Zhang, J., & Li, X. (2023). How do risks and benefits affect user' privacy decisions? An event-related potential study on privacy calculus process. *Frontiers in Psychology*, *14*, 1052782. https://doi.org/10.3389/fpsyg.2023.1052782

Goldfarb, A., & Tucker, C. (2011). Shifts in Privacy Concerns. *American Economic Review*, *102*. https://doi.org/10.2139/ssrn.1976321

Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, *87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x

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

Herr, P., Page, C., Pfeiffer, B., & Davis, D. (2012). Affective Influences on Evaluative Processing. *Journal of Consumer Research*, *38*, 833–845. https://doi.org/10.1086/660844

Hodson, T. (2022). Root-mean-square error (RMSE) or mean absolute error (MAE): when to use them or not. *Geoscientific Model Development*, *15*, 5481–5487. https://doi.org/10.5194/gmd-15-5481-2022

Japec, L., Kreuter, F., Berg, M., Biemer, P., Decker, P., Lampe, C., Lane, J., O'Neil, C., & Usher, A. (2015). Big Data in Survey Research. *Public Opinion Quarterly*, *79*, 839–880. https://doi.org/10.1093/poq/nfv039

Karunasingha, D. S. K. (2022). Root mean square error or mean absolute error? Use their ratio as well. *Information Sciences*, *585*, 609–629. https://doi.org/https://doi.org/10.1016/j.ins.2021.11.036

Keskin, B. (2013). *Statistical Power Analysis*.

Kim, Y., Kim, S. H., Peterson, R. A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. *Technological Forecasting and Social Change*, *196*, 122789. https://doi.org/https://doi.org/10.1016/j.techfore.2023.122789

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*. https://doi.org/10.1016/j.cose.2015.07.002

Le, T.-T., Lin, P.-T., Duc, D. T. V., Dang, T.-Q., & Nguyen, L.-T. (2025). Optimizing and restructuring resources for sustainable firm performance in the AI era: the role of dynamic capabilities and circular manufacturing. *Sustainable Futures*, *10*, 101441. https://doi.org/10.1016/j.sftr.2025.101441

Li, Z., Choi, M., & Kim, H.-E. (2025). AI Awareness and Employee Innovation: A Dual-Pathway Moderated Mediation Model Within Organizational Systems. *Systems*, *13*, 530. https://doi.org/10.3390/systems13070530

Lwin, M., Williams, J., & Wirtz, J. (2007). Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science*, *35*, 572–585. https://doi.org/10.1007/s11747-006-0003-3

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

Mark, M., & Henry, G. (2004). The Mechanisms and Outcomes of Evaluation Influence. *Evaluation*, *10*, 35–57. https://doi.org/10.1177/1356389004042326

Martin, K., Borah, A., & Palmatier, R. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*. https://doi.org/10.1509/jm.15.0497

Motsenok, M., Kogut, T., & Ritov, I. (2021). Perceived Physical Vulnerability Promotes Prosocial Behavior. *Personality and Social Psychology Bulletin*, *48*. https://doi.org/10.1177/01461672211005879

Palmer, V. (2007). Narrative Repair: [Re]covery, Vulnerability, Service, and Suffering. *Illness, Crisis, & Loss*, *15*, 371–388. https://doi.org/10.2190/IL.15.4.f

Pavlou, P., & Gefen, D. (2004). Building Effective Online Marketplaces with

Institution-Based Trust. *Information Systems Research*, *15*, 37–59. https://doi.org/10.1287/isre.1040.0015

Phan, L.-G. N., Tri, D. Q., Dang, S.-H., & Nguyen, L.-T. (2025). Hooked on Livestreaming: What Drives Customer Repurchase Intention in E-Commerce? *Journal of Creative Communications*. https://doi.org/10.1177/09732586241311001

Rosenau, J. N. (1984). A Pre-Theory Revisited: World Politics in an Era of Cascading Interdependence. *International Studies Quarterly*, *28*(3), 245–305. https://doi.org/10.2307/2600632

RUBACI, H., & AKGÜL, Y. (2019). DIGITAL CUSTOMER ENGAGEMENT DIMENSIONS IN DIGITAL TRANSFORMATION AND A FRAMEWORK SUGGESTION FOR RETAIL BANKING. *Journal of Life Economics*, *6*, 239–248. https://doi.org/10.15637/jlecon.6.014

Russo, G., Tomei, P., Serra, B., & Mello, S. (2021). Differences in the Use of 5- or 7-point Likert Scale: An Application in Food Safety Culture. *Organizational Cultures: An International Journal*, *21*, 1–17. https://doi.org/10.18848/2327-8013/CGP/v21i02/1-17

Schrader, P. G., & Lawless, K. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. *Performance Improvement*, *43*, 8–15. https://doi.org/10.1002/pfi.4140430905

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management*, *50*(1), 1–12. https://doi.org/https://doi.org/10.1016/j.im.2012.11.002

Sloan, R., & Warner, R. (2016). *Unauthorized Access: The Crisis in Online Privacy and Security*. https://doi.org/10.1201/b15148

Smith, H., Dinev, T., & Xu, H. (2011a). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*, 989–1015. https://doi.org/10.2307/41409970

Smith, H., Dinev, T., & Xu, H. (2011b). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*, 989–1015. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices1. *Management Information Systems Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Steindl, C., Jonas, E., Sittenthaler, S., Traut-Mattausch, E., & Greenberg, J. L. (2015). Understanding Psychological Reactance. *Zeitschrift Fur Psychologie*, *223*, 205–214. https://api.semanticscholar.org/CorpusID:18944273

Tien, P. C. T., Luan, N. T., & Tri, D. Q. (2023). Exploring the brand experience of Korean brands on customer interactions in Ho Chi Minh City, Vietnam: non-linear structural equation modelling approach. In T. Van Tieng (Ed.), *Kỷ yếu hội thảo khoa học quốc tế Việt - Ha\`n 2023* (pp. 276–289). Information and Communications Publishing House; ZBW - Leibniz Information Centre for Economics. https://hdl.handle.net/10419/278122

van der Pligt, J. (2001). Vulnerability and Perceived Susceptibility, Psychology of. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 16333–16335). Pergamon. https://doi.org/https://doi.org/10.1016/B0-08-043076-7/03807-9

Vives, X. (2019). Digital Disruption in Banking. *Annual Review of Financial Economics*, *11*, 243–272. https://doi.org/10.1146/annurev-financial-100719-120854

Wirtz, J., Lwin, M., & Williams, J. (2007). Causes and Consequences of Consumer Online Privacy Concern. *International Journal of Service Industry Management*, *18*, 326–348. https://doi.org/10.1108/09564230710778128

Zhao, H., Fu, C., Zhang, Y., Zhu, W., Lu, K., & Francis, E. M. (2024). Dimensional decomposition-aided metamodels for uncertainty quantification and optimization in engineering: A review. *Computer Methods in Applied Mechanics and Engineering*, *428*, 117098. https://doi.org/https://doi.org/10.1016/j.cma.2024.117098