

# Antecedents of Consumers' Privacy Protection Behavior and Intention to Disclose Personal Information: Mediating Role of Personal Information Transparency

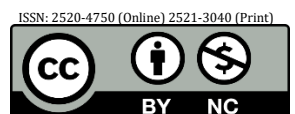
Sefora Hailu Yoseph & Gao Chongyan

## Abstract

Online platforms have exhibited several perceived and actual challenges to privacy. Using a complex research model, this study examines direct, mediating, and moderating effects on several privacy variables. It involved 335 respondents using systematic random sampling from online consumers and hypotheses testing using structural equation modeling. The antecedents of consumers' intention to disclose personal information were confirmed for privacy vulnerability and privacy benefit. On the other hand, the antecedent of consumers' privacy protection behavior in relation to privacy vulnerability was found to be statistically insignificant but confirming privacy benefits. As predicted, the mediating roles of privacy information transparency were proven empirically, and so were the moderating roles of privacy cynicism. This research addresses research gaps suggested by previous esteemed scholars and suggests several guidelines for practitioners. Finally, it outlined core research themes for future researchers.



IJSB  
Accepted 12 June 2024  
Published 16 June 2024  
DOI: 10.58970/IJSB.2388



Papers published by IJSAB International are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

**Keywords:** *Privacy Vulnerability, Privacy Benefits, Privacy information, Transparency Privacy, Cynicism, Intention to disclose personal information, Privacy protection behavior.*

## About Author (s)

**Sefora Hailu Yoseph**, PhD Candidate, Business School, International Marketing, University of International Business and Economics (UIBE), Beijing, China.

**Gao Chongyan** (Corresponding author), Associate Professor, Business School, International Marketing, University of International Business and Economics (UIBE), Beijing, China.

## I. Introduction

Businesses nowadays are more likely than ever to connect with a wide range of consumers online (Cho and Sutton, 2021). In addition to raising concerns about privacy invasions and breaches that have an impact on customers' well-being, the platforms are a useful tool for communicating client-business relationships (Watanabe et al., 2021). Establishments anticipate handling major customer disclosures of personal information, but privacy vulnerabilities can significantly influence consumers' intentions to share information or take preventive measures to safeguard their privacy. Despite the ease, efficacy, and efficiency of e-business, concerns about privacy vulnerability, security, susceptibility, and instability are impacting people's lives, whether to disclose personal information or apply protective behavior. Practitioners' interest in the topic has spurred studies on the causes and effects of consumers' privacy management. The impact of privacy vulnerability and privacy benefits has been largely ignored in the varied results of existing empirical investigations that attempt to identify antecedents of privacy protection behavior and consumers' intentions to disclose personal information. Thus, this research aims to address a number of research calls (see Table 1). For example, numerous researchers have suggested that future research should focus on understanding how web design builds confidence in minimizing risks, users' cynicism, control, and the context of e-commerce, while also emphasizing the generalizability of research findings (Agozie & Nat, 2020; Choi, 2020; Kim et al., 2019). We should also address the call for research on privacy protection behavior, the intention to disclose personal information that includes multiple factors, and its impact on personality traits (Jin, 2022; Alzaidi & Agag, 2022). Furthermore, there are extensive ambivalences in studies regarding privacy vulnerability, benefits, e-commerce reputation and design, including disclosure, cynicism, and privacy concerns (Agozie & Nat, 2020; Choi, 2020; Kim et al., 2019; Alzaidi & Agag, 2022; Jin, 2022). Likewise, De Wolf (2020); Dunbar et al. (2021); Liu B. (2022); Acikgoz and Vega (2022); and Van Ooijen et al. (2022) studies provide mounting evidence of privacy vulnerability and benefits on online platforms, underscoring the critical need to address this research.

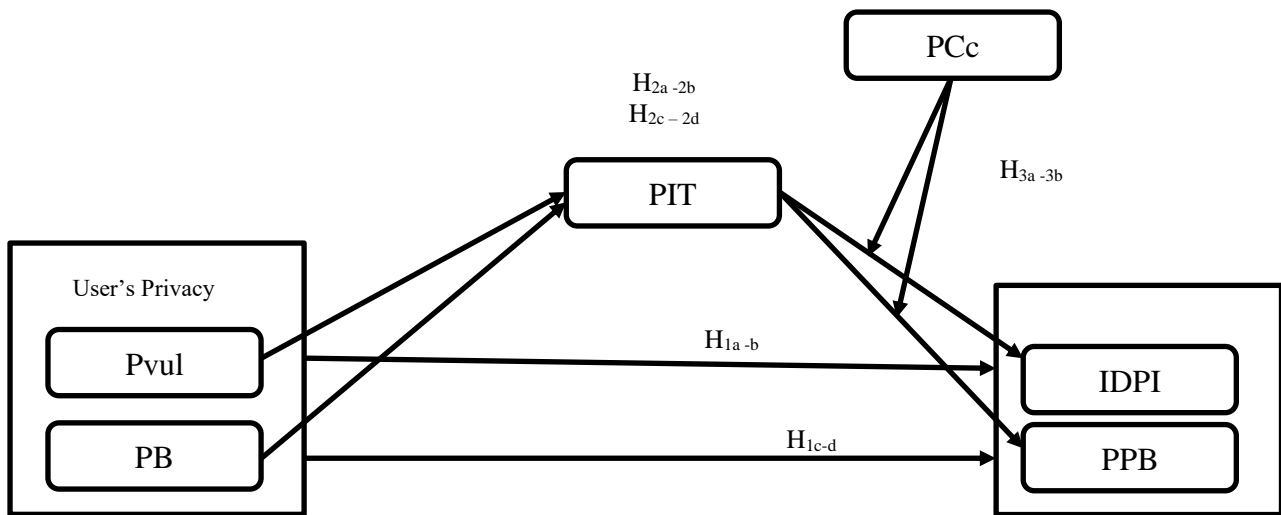
Data breach events have persisted despite ongoing attempts to safeguard users' privacy rights (Sen & Borle, 2015). Chin (2023) revealed the largest data breach in US history. For instance, Yahoo had 3 million users between 2013 - 2016, which resulted in a \$35 million fine, and Microsoft faced 60 thousand companywide cyberattacks and hackers in January 2021 that the company couldn't push to fix the situation for months. Therefore, examining the impact of privacy vulnerability and privacy benefits would not only expand knowledge on privacy protection behavior (intention to disclose personal information) but also provide practical guidance for online platform operators. While personalization has many advantages for businesses, including fostering customer loyalty (Martin et al., 2017) and increasing retail sales (Luo et al., 2020), it has also created a dilemma for consumers' personalization-privacy paradox (Sutanto et al., 2013). Customers may find online personalization advantageous, on the one hand, since tailored promotions take their preferences into account as a value of personalization. However, when customers face inappropriate and unauthorized transgressions of personal information—that is, the intrusion of personalization—they may feel uneasy and apprehensive (Martin et al., 2017), which may hamper consumers' intention to disclose personal information or affect their online protection behavior. Against this background, we conceptualize and test antecedents of privacy protection behavior (intention to disclose personal information), defined as the degree to which consumers perceive privacy vulnerability and benefits on online platforms. We also tested the intervening role of personal information transparency between privacy vulnerability (benefit) and outcome variables, consumers' privacy protection behavior, and their intention to disclose personal information.

We have further examined how consumers' privacy cynicism moderates the relationship between the intervening and outcome variables (see Figure 1).

**Table 1: Related Literature and Research Gaps**

Author (s)/ year/ Journal	Title	Research Implications	Proposed variable (s) and/or Implications to this study
Acikgoz and Vega, 2022; International Journal of Human-Computer Interaction	The role of privacy cynicism in consumer habits with voice assistants: a technology acceptance model perspective.	Deepening the research on behavioral influence of privacy cynicism, privacy concern, hedonic use of voice assistant (VA), and AI-based technologies with association of mediation variables. In addition, it was suggested to adopt theories of Expectation Confirmation Theory (ECT) and Diffusion of Innovation Theory (DIT) for analysis.	Privacy cynicism Personal Information Transparency
Agozie and Kaya, 2021; Inf. Q.	Discerning the effect of privacy information transparency on privacy fatigue in e-government.	Investigation is demanded on privacy assurance, service platform's design (structure, word choice, organization), and reactions to privacy behavior, and privacy fatigue.	Personal information transparency Privacy protective behavior
De Wolf, 2020; New Media Soc.	Contextualizing how teens manage personal and interpersonal privacy on social media.	Future study recommended on severity and recency turbulence of privacy management, privacy concern, and context-related such communicative system, security, consent, fatigue or breach relations to examine privacy behavior.	Privacy vulnerability
Dunbar et al., 2021; Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.	Is Someone Listening? Audio-Related Privacy Perceptions and Design Recommendations from Guardians, Pragmatists, and Cynics. Proc.	Heightening our scope on privacy needs and vulnerabilities, privacy issues related to other than US geographic context, privacy paradox such attitude and actions of end-users. It is also recommended to assess facts privacy from platform design protocols and cynicisms.	Privacy vulnerability Privacy cynicism
Liu B., 2022; Journal of Modern Information	Study on the influence mechanism of user's information privacy behavior from the perspectives of both technical characteristics and individual difference	Future study is expected to address non-young consumers for generalizability, include technical characteristics and individual difference, other factors that affect privacy fatigue, and examine the discrepancy between intention and actual privacy behavior.	Privacy vulnerability Perceived benefit Privacy cynicism Intention to disclose personal information
Van Ooijen et al., 2022; Communication Research	Privacy cynicism and its role in privacy decision-making.	Examining the role of privacy perceived severity and self-efficacy in privacy-protection behavior; privacy cost-benefit models, and individual difference in attitude (vulnerability, benefit) behavior.	Privacy Vulnerability Privacy Benefit Privacy protection behavior

Recent privacy studies (Van Ooijen et al., 2022; Liu, 2022; Tang et al., 2020; Acikgoz and Vega, 2022; Dunbar et al., 2021) shed light on privacy behaviors that provide mixed evidence on how to protect privacy or resist consumers' temptation to disclose personal information. As a result, the study aims to investigate whether privacy vulnerability and privacy benefit may act as antecedents to consumers' intention to disclose personal information, thereby contributing to the existing literature on privacy protection behavior. Considering privacy information transparency that helps unlock the platform's operation, service offerings, and process information aspects (Zhou et al., 2018), we examine the mediating role of privacy information transparency in consumers' decision-making that ultimately leads to privacy management. Critically viewing research linking mistrust and privacy skepticism (Lutz et al., 2020) of online platforms, we examine how consumers' privacy cynicism interaction effects privacy information transparency and both consumers' privacy protection behavior and intention to disclose personal information.



**Figure 1: Conceptual Model**

**N.B.** *Pvul* = Privacy Vulnerability, *PB* = Privacy Benefits, *PIT* = Privacy Information Transparency, *PCc* = Privacy Cynicism, *IDPI* = Intention to Disclose Personal Information, and *PPB* = Privacy protection behavior.

The research contributes to the privacy literature in three ways. First, increasing consumers' perceptions of privacy vulnerability has an effect on consumers' privacy decisions, such as privacy susceptibility (Hameed & Arachchilage, 2019); privacy hazards (Dinev & Hart, 2004); and online theft and fraud impacting privacy intentions (LaRose & Rifon, 2007). Thus, it is critical to advance our insights on how perceived privacy vulnerability impacts consumers' intentions to disclose personal information and/or privacy protection behavior. Similarly, implications of consumers' perceived privacy benefits in adapting privacy behavior include utilitarian value (Yang & Lee, 2019); usefulness (Davis, 1989, 1993); degree of satisfaction (Moriuchi, 2019); and prerequisites to technological adoption (Burke, 1997). Therefore, it is important to advance knowledge on the extent to which perceived privacy benefits influence consumers' intentions to disclose personal information (privacy protection behavior). Second, research has addressed several ambivalences on the relevance of information transparency and privacy assurance. For example, privacy information transparency leads to privacy assurance (Ibrahim & Narcyz, 2015; Xu et al., 2011); the fundamental construct of privacy management and rationale for privacy trust (Choi et al., 2018); and input to unlock the platform's operation (Zhou et al., 2018). This study investigates the intervening role of privacy information transparency, which could potentially play on contradictory assertions between privacy vulnerability (benefit) and consumers' intention to disclose personal information (privacy protection behavior). Finally, taking into account the role of privacy cynicism in creating or fostering mistrust (Boush et al., 1993; Regoli, 1976), unfulfilled expectations (Thompson et al., 1999), and unachievable privacy standards (Choi et al., 2018; Lutz et al., 2020), we can explore the possibility that privacy cynicism plays a moderating role between privacy information transparency and both outcome variables (consumers' privacy protection behavior and their intention to disclose personal information). This work will provide empirical evidence on the role of privacy cynicism in consumers' privacy decision-making and behavior when interacting with online platforms.

## II. Theoretical Framework and Hypothesis Development

Current prevailing privacy challenges require extensive effort and in depth understanding of the drivers and contexts privacy protection behavior (intention to disclose personal information). Existing research design of privacy management (Van Ooijen et al., 2022), privacy

behavior (Liu, 2022), privacy perceptions (Dunbar et al., 2021), have displayed useful conceptualization; yet, the studies remain to uncover privacy vulnerability (benefit) antecedental role of consumers' privacy protection behavior (intention to disclose personal information), mediation role of personal information transparency, and moderation effect of privacy cynicism. In the next sections, we build conceptualization and hypotheses development of privacy protection behavior, intention to disclose personal information, privacy vulnerability, benefit, personal information transparency, and privacy cynicism.

### ***Privacy Protection Behavior (PPB)***

Consumers tend to develop privacy protective behavior to maximize the gains of online exposure. When customers become more conscious of the different privacy conflicts that arise during business dealings, their anxiety or dread may lead them to take preventive measures (Walker, 2016). The type of resources and regulations accessible in their partnerships with firms determine how much dread or stress they experience. Relationship structure assessments probably take into account the degree of privacy concerns, how likely they are to occur, and how vulnerable or empowered the individual feels to manage those risks (Lwin et al., 2007). Customers are more likely to engage in privacy-protective behaviors, which show up as future reactions to the structures and resources available within that relationship, if they are aware of increased privacy risks resulting from, for instance, the nature of the data being collected or increased breach likelihood in a firm relationship. Certain privacy-protective behavior provides users' control over their personal data (e.g., reducing disclosures, minimizing their digital footprint) or mandate express consent before using their data on information access and use (Walker, 2016). As a result, it is critical time to distinguish between proactive and reactive defense tactics. When customers choose a proactive approach, they anticipate privacy risks and take appropriate action; when they adopt a reactive approach, they follow a company's explicit advice or react to an urgent threat. According to Quach et al. (2022) the reactive/proactive and information control/permission control dimensions are thus covered by two-dimensional categorization of consumer privacy protection behavior, which results in four groups: (1) reactive information strategy, (2) proactive information strategy, (3) reactive permission strategy, and (4) proactive permission strategy.

### ***Intention to Disclose Personal Information (IDPI)***

Consumers' decision regarding whether to disclose data depend on policies how the data is captured, utilized, or transferred as firms authentic right of online platforms. Zeng et al. (2020) note the existing research on self-disclosure can be categorized into two streams - one focused on its association with intimacy and trust (Moon, 2000), and how interviewees' characteristics influenced self-disclosure intentions (Utz, 2015). Issues remain unanswered on the outcomes and determinants of self-disclosure influences on customer purchase as well as the key privacy policies used to motivate the self-disclosure. Self-disclosure is a manifestation of authorization to view and access data as well as a signal of one's willingness to increase intimacy and develop a close, reciprocal, and interactive relationship (Cozby, 1973). The commitment to disclose one's personal data implies that the customer authorizes the firm to access the details that they have provided. However, it assumes that customers can precisely identify whether the data used in subsequent personalized promotions, personalized content based on self-disclosure data increases customers' perceived control and decreases perceived privacy risks, which may induce compliance with personalized promotion. Level of commitment to self-disclosure at the initial stage implies the customer's willingness to build a close, reciprocal, and interactive relationship with the firm (Cozby, 1973), which will induce strong trust in the firm and its perceived attractiveness (Moon, 2000). As personalized products and services satisfy customers' willingness to receive additional exchange values by better targeting their needs

and interests (Goldfarb & Tucker, 2011), self-disclosure customers are more likely to make a purchase at the personalized promotion stage. However, inconsistency between the explicit self-disclosure refusal and the later personalized promotion results in perceived vulnerability and intrusiveness (Martin et al., 2017), subsequently triggering privacy concerns and discouraging purchase responses to personalized promotions (Aguirre et al., 2015).

### ***Privacy Vulnerability (Pvul)***

Consumers' privacy vulnerability occurs due to supposedly downsides of information disclosure, online fraud, theft, risks, and susceptibility to breaches on privacy data. According to Dinev and Hart (2004), vulnerability to privacy risks refers to the alleged drawbacks of information disclosure. LaRose and Rifon (2007) found that customers' expectations of negative outcomes—like online fraud or identity theft—were positively correlated with their privacy concerns in their study of adult consumers. According to research by Norberg, et al., (2007), consumers' intentions to give personal information to a marketer were negatively impacted by their impression of the overall risk associated with information disclosure. Dinev and Hart (2004) found a positive correlation between privacy concerns and perceived vulnerability to privacy hazards. The perceived seriousness of a data breach and an individual's susceptibility to such an occurrence influence the motivation for data protection in our security setting. According to Hameed & Arachchilage, (2019), a person's perceived vulnerability is their level of susceptibility to a threat. Higher susceptibility individuals are more aware of the need for information system security protection. According to Lee and Larsen (2009), a person's intention to use security technologies is significantly influenced by their perception of vulnerability. Adoption and behavior related to information security have been found to be generally influenced by the perception of threat susceptibility (Ifinedo, 2012; Ng et al., 2009, Stanton et al., 2005). Additionally, the intention to avoid information system security threats is positively influenced by perceived vulnerability (Hameed & Arachchilage, 2019). According to a number of studies, people are more inclined to take precautionary action if they believe that their information security assets are at risk of being attacked (Hanus & Wu, 2016; Meso et al., 2013; Tu et al., 2018). Thus, we can hypothesize that consumers' privacy vulnerability and benefit may be the antecedents of both consumers' privacy protection behavior and their intention to disclose personal information.

***H1a: Consumers' perceived privacy vulnerability (Pvul) is positively related to intention to disclose personal information (IDPI).***

***H1b: Consumers' perceived privacy vulnerability (Pvul) is positively related to privacy protection behavior (PPB).***

### ***Privacy Benefit (PB)***

Perceived benefit depends on consumers' opinion of technology labelled as perceived usefulness, and a belief about the behavioral intention (Davis, 1989, 1993). According to Moriuchi (2019), perceived benefits may have an impact on an attitude or degree of satisfaction that is based on psychological or sociological theories. This is because, according to Burke (1997), perceived benefit is one of the main prerequisites for technological adoption. Conceptually, perceived usefulness is connected to utilitarian value, which denotes customer value derived from features with a focus on function (Yang & Lee, 2019). More data supports this theory by demonstrating how technology can improve and simplify consumers' daily life (Ofori et al., 2016). Previous research backs up the idea of perceived usefulness that one factor influencing attitudes toward technology and behavioral intentions. For example, perceived benefit has been studied by Walter and Abendroth (2020) as a functional benefit in the development of a favorable attitude toward in-vehicle connected services. In addition, a number of studies have looked into how attitudes and usage intentions are affected by

perceived usefulness in various contexts, including intentions to use smartphones (Park & Chen, 2007), adopt mobile internet (Kim et al., 2007), and engage in online shopping (Fortes & Rita, 2016). Thus, privacy benefit may act as antecedents of both outcomes, we posit that:

**H<sub>1c</sub>:** *Consumers' perceived privacy benefit (PB) is positively associated with the intention to disclose personal information (IDPI).*

**H<sub>1a</sub>:** *Consumers' perceived privacy benefit (PB) is negatively related to privacy protection behavior (PPB).*

### **Mediation Test of Personal Information Transparency (PIT)**

Consumers tend to provide their personal information transparently when the feelings of fear of online system are minimized or their confidence feelings are uplifted. Numerous researches have addressed the relevance of information transparency, which is a fundamental notion in privacy assurance (Ibrahim & Narczyk, 2015; Xu et al., 2011). Transparency in various contexts, such as recommender of systems and search engines, for example, shows a system that makes it easier for users to comprehend how these systems operate. Users perceive these systems as transparent since they are provided with explanations and reasoning for the search recommendations and results (Choi et al., 2018; Ibrahim & Narczyk, 2015). Comparably, information transparency helps to unlock the platform's operation, service offerings, and process information aspects (Zhou et al., 2018; Xu et al., 2014) that this is achieved through making platform information available and accessible. In light of the primary facets of user information management, this may thus satisfy users' information needs (Xu et al., 2014). The consensus across studies on transparency is that easily comprehensible and available information meets consumers' information needs (Xu et al., 2011). According to Gupta et al. (2020), the idea of information transparency has a strong foundation and relevance in e-platforms. According to Zhou et al. (2018), consumers start to worry about how much personal information is revealed if they believe they have the desired level of control over information exchanges. As a result, consumers' information transparency is expected to intervene the relations between privacy vulnerability (benefit) and both outcome variables. Specifically,

**H<sub>2a</sub>:** *Consumers' personal information transparency mediates the relations between perceived privacy vulnerability (Pvul) and their intention to disclose personal information (IDPI).*

**H<sub>2b</sub>:** *Consumers' personal information transparency mediates the relations between consumers' perceived privacy vulnerability (Pvul) their privacy protection behavior (PPB).*

**H<sub>2c</sub>:** *Consumers' personal information transparency mediates the relations between perceived privacy benefit (PB) and their intention to disclose personal information (IDPI).*

**H<sub>2a</sub>:** *Consumers' personal information transparency mediates the relations between consumers' perceived privacy benefit (PB) their privacy protection behavior (PPB).*

### **Moderation Effect of Privacy Cynicism (PCc)**

Consumers can develop privacy cynicism due to negative feelings, disappointment, excessive feelings of threat, and unfulfilled expectation in using online platforms. Cynicism can be caused by negative feelings and beliefs about any issue or system (Andersson, 1996; Choi et al., 2018). Cynicism mostly intensifies unfulfilled expectations in every situation where an individual is faced with hardship, hopelessness, or disappointing situations (Choi et al., 2018, Lutz et al., 2020). According to theory, cynicism results from idea or experience misalignment that breeds mistrust in a variety of contexts (Boush et al., 1993; Regoli, 1976). Numerous writers point out that obstacles and unmet expectations can lead to mistrust (Thompson et al., 1999); mistrust can also result from unmet requirements and unachievable standards (Choi et al., 2018). Furthermore, research shows a link between mistrust and privacy skepticism (Lutz et al., 2020). As a result, whether or not cynicism acknowledges detrimental preconditions to trust development comes into play. Dean et al. (1998) defined cynicism as a negative attitude toward

one's employer or institution as well as the company as a whole in the literature on organizational management. This definition bears similarities to the notion of mistrust concerns. Furthermore, skepticism is thought to represent a lack of confidence in an institution's system (Bateman et al., 1992). A further perspective on cynicism is the way that people's growing skepticism affects their views toward adopting and using mobile banking (Chaouali et al., 2017) and other e-service platforms. Against this background, we posit that weaker privacy cynicism provides a weaker personal information transparency and consumers' intention to disclose personal information. The higher privacy cynicism, on the other hand, stronger effect between consumer's information transparency and their privacy protective behavior.

**H<sub>3a</sub>:** *The relationship between privacy information transparency (PIT) and consumers' intention to disclose personal information (IDPI) will decline when there is weak influence of privacy cynicism (PCc).*

**H<sub>3b</sub>:** *The impact of privacy information transparency (PIT) on consumers' perceived privacy protection (PPB) will be higher when there is high influence of privacy cynicism (PCc).*

### III. Methodology

#### **Design**

Research design is a comprehensive strategic outline of how a researcher intends to find research participants and get data from them (Welman and Kruger, 2005), with a view to sampling methods and the associated survey strategy. The study aims to collect data from a large population using probability sampling that fairly represents the population under study for the purposes of generalizability. As regards the web-based survey, Couper (2000: 465–466) perhaps said it best: "...web-survey approach must be done in the context of its intended purpose and the claims it makes." Cross-sectional data is generalizable based on individual or group observations and facilitates the economical collection of data from a population (Saunders et al., 2009). Depending on the goals of the study, each system can use exploratory, descriptive, or explanatory research (Yin, 2003); thus, the study's goals prescribe an explanatory survey to determine the causal influence of the mediated and moderated interactions (Saunders et al., 2009). Around 36.8 million consumers use the Tele Birr app, out of which over 25% (expert opinion) of those subscribers reside in the capital, Addis Ababa. The company, using media reports, reports that the study's population is around 1.4 million online service users, comprising 1.08 trillion transactional values in 2023. According to Saunders et al. (2009), the sampling frame should provide a comprehensive, current, and precise depiction of all the cases the study aims to investigate, allowing for accurate sampling. Although targeting the entire population could be interesting, it is unrealistic due to time and budget constraints. In line with the literature, when a sampling frame is unavailable, researchers can set up a sampling frame for the specific study, ensuring validity (Saunders et al., 2012); undertake marketing research at less cost from a population even when the sampling frame is indefinite (Kotler & Armstrong, 2015).

#### **Sampling and Data Collection Procedures**

The study aims to use non-list-based random sampling to implement probability sampling, avoiding the traditional practice of enumerating the sampling frame known as random digital dialing (RDD) in telephone surveys. The RDD couldn't fit into a web-based survey, and thus, the intercept survey (Saunders, 2014; Dillman et al. (2014); Walgrave and Verhulst, 2011) frequently uses systematic sampling of visitors from online vendors, online service providers, and shopping malls. Systemic random sampling, where the initial sampling point is selected at random and then the next customer is selected at a regular interval using the intercept survey approach (Couper, 2000), Following the capital geographic location that divides into ten sub-



cities (Bole, Yeka, Akaki-kaliti, Nfas Silk, Kolfe-Keranio, Gullel, Addis Ketema, Arada, Lideta, and Krkos), the researcher opts to establish four research panels: North East (NE), South East (SE), North West (NW), and South West (SW), and also delineates targets at each panel: a shopping mall, a gas station, and a utility, say electric bills. Twelve research assistants were recruited from Addis Ababa University students to work in the four research panels (NE, NW, SE, and SW), with an equal workload of recruiting 115–116 respondents each. Each research panel assigns three research assistants to predetermined e-service providers. The expected sample was 462, and we received 335 consumers' data (73% response rate) at a female-to-male ratio of 49:51. The response rate for online surveys was higher than the 50% suggested by Mendenhall and colleagues (2003), ranging from 35% to 47% for Dillman's (2007) and Ballantyne's (2005) surveys. The researcher's data collectors were trained to pick the first customer, and then the next intercept customer to be the fifth, 10<sup>th</sup>, 15<sup>th</sup>, and so forth for 8 working hours for consecutive five days at their respective assigned e-service provider, in line with the literature review, for instance, Dillman et al. (2014), Saunders (2014), Walgrave and Verhulst (2011), and others who recommend the intercept sampling approach as a feasible and advantageous method given the opportunity to win consent and customers' willingness to participate in the survey. The researchers recommend a pattern of five plus one for non-willing customers; if that customer again declines, they instruct the research assistants to move on to the next eligible (regular fifth) customer during the training session.

### ***Instruments***

A critical literature review was made against the study's variables. Following Ghauri and Grønhaug (2010) recommendations while constructing the questionnaire, a critical evaluation of the literature was made on the variables to establish measurements and assume significant correlations between the variables. The variables were derived from previous studies, and the survey items were slightly modified in relation to the specific research need. Using a five-point Likert scale representing "strongly agree" to "strongly disagree," that provides consumers with a rating in relation to their perceptions and/or experience with using online platforms. The five questionnaire items of privacy vulnerability are adapted from Dinev and Hart (2006); three items of privacy benefit from van Ooijen et al. (2022); personal information transparency's four items from Agozie & Kaya (2021); three items of privacy cynicism from Choi et al. (2018); intention to disclose personal information measured using three items suggested by Malhotra et al. (2004); and adapted privacy protection behavior six items from Park & Mo Jang (2014); Wottrich et. al. (2019).

## **IV. Empirical Results**

### ***Descriptive Statistics***

Table 2 reports the descriptive statistics and bivariate correlations for independents, mediator, moderator, controls, and outcome variables. The standard deviation for age is 9.7, indicating a higher dispersion of data in relation to its mean, specifically in the range of 18 to 71 years. The controlling variables indicate the controlling effect on the study's variables. As expected, perceived privacy benefit (e.g.,  $r = .26$ ,  $p = .01$ ) and personal information transparency (e.g.,  $r = .20$ ,  $p = .01$ ) significantly correlate with the outcome variables: consumers' intention to disclose personal information and privacy protection behavior, implying the direction and extent of relationships. The independent variables privacy vulnerability and privacy benefit ( $r = .17$ ,  $p = .01$ ) have a significant correlation, indicating that both are statistically related. As correlation doesn't mean causation, privacy vulnerability was found to have an insignificant correlation with the outcome variable (e.g.,  $r = .10$ ,  $p < .05$ ), leaving room for further investigation.

**Table 2: Descriptive statistics and Pearson’s Correlations (N = 335)**

	Mean	Std. Deviation	N	Av_Pvul	Av_PB	Av_PCc	Av_PIT	Av_IDP I	Av_PP B	Sex	Age	Marital
Av_Pvul	3.25	1.77	335	1								
Av_PB	4.28	0.98	335	.166**	1							
Av_PCc	2.48	1.48	335	.235**	.036	1						
Av_PIT	3.51	1.10	335	-.138*	-.170**	.108*	1					
Av_IDP I	3.43	1.24	335	.104	.256**	.130*	.133*	1				
Av_PP B	3.23	0.93	335	.015	-.178**	-.029	.201**	-.187**	1			
Sex	1.51	.501	335	.201**	.173**	-.016	-.012	.027	-.008	1		
Age	37.36	9.67	335	.105	.111*	.026	.171**	.125*	.002	-.012	1	
Marital	1.82	.850	335	.067	.162**	-.011	.178**	.187**	-.036	-.101	.464*	1

\*\*.

Correlation is significant at the 0.01 level (2-tailed).

\*.

Correlation is significant at the 0.05 level (2-tailed).

**V. Data Analysis**

**Reliability and Validity Tests**

In the first step, the Explanatory Factor Analysis (EFA) using the communality extraction factor shows the item variance in factor loading (Brown, 2015). The acceptable communality cutoff measure was suggested between .25 to .4 and the ideal communality range falls 0.7 and above (Beavers et al., 2013). According to Annex 1, twenty out of twenty-three stands on ideal communalities, and the remaining three (PB1 =.65, PIT1 =.52, and PPB2 =.65) recorded slightly below the ideal cutoff but above the suggested acceptable range. For reliability tests, Cronbach’s alpha (α) value is 0.7 and above, which indicates the reliability of the constructs (Hair et al., 2010).

Fornell and Larcker (1981) proposed further analysis. These are: 1) the standardized regression weight exceeds 0.7 at the p <.05 or p <.01 significance level; 2) construct reliability (CR) exceeds the 0.7 threshold; and 3) the average variance extracted (AVE) estimates the variance between latent indicators greater than 0.6. As Annex 1, the standardized factor loading of nineteen out of twenty-three items is above the cut-off value of 0.7, and three items are close to this threshold considering the variables’ number of items. Therefore, the analytical procedure recommends the deletion of item PPB2 due to its below-standard performance. As depicted in the Annex 1, the values of construct reliability (CR) range from 0.85 to 0.98 within the recommended threshold, and the average variance extracted (AVE) is above the proposed value of prior literature. Therefore, this analysis infers the eligibility of convergent validity, which paves the way for discriminant validity. In view of analyzing discriminant validity, it requires examination of both the EFA and the CFA. Initially, the sample adequacy test using the Kaiser-Meyer-Olkin (KMO) assesses the sample’s ability to place the items onto factors (Kaiser, 1974). KMO values ranging from above the 0.8 to 0.6 cutoff (Beavers et. al., 2013) are standard indicators to confirm or decline sample adequacy. The outcome indicates within the preferred range (.717) and Bartlett’s Test of Sphericity approximation Chi-Square 8896.57, degree of freedom of 276, and p-value =.000, proving an eligible sample size. The estimates of factor loading coefficient of the entire items of the constructs exceed 0.7, and the cumulative variance of interpretation rate after rotation of seven items is 85.27%, over 50% of the of the recommended value, which implies the research data is effectively extracted. In addition, each square root of AVE is greater than the correlation coefficient (Table 3), supplementing to prove discriminant validity (Fornell and Larcker, 1981). Both pieces of evidence are sufficient conditions to approve measurement items discriminant validity.

**Table 3: Pearson's Correlation and Square Root of AVE**

	Av_Pvul	Av_PB	Av_PCc	Av_PIT	Av_IDPI	Av_PPb
Av_Pvul	<i>.926</i>					
Av_PB	.166**	<i>.817</i>				
Av_PCc	.235**	.036	<i>.896</i>			
Av_PIT	-.138*	-.170**	.108*	<i>.771</i>		
Av_IDPI	.104	.256**	.130*	.133*	<i>.910</i>	
Av_PPb	.015	-.178**	-.029	.201**	-.187**	<i>.774</i>
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

N.B. The diagonal italicized values are the square root of AVE

### Analysis of Common Methods Variance

Behavioral research may face difficulties due to common method variance (CMV) (Podsakoff et al., 2003). It confirms whether or not there is any noise on the instrument (Chang and Eden, 2010). We examined the study's variables—privacy vulnerability, benefit, cynicism, transparency of personal information, consumers' intention to disclose personal information, and their privacy-protective behavior—to assess a common factor. Following the Podsakoff et al.'s recommendation to conduct an EFA test of common method bias using Harman's single component analysis, the maximum variance in this study was 23.71% on any one factor. The suggested overall variance for a single factor shouldn't exceed 50% and hence, the results suggest that there are no CMV- problems with the dataset for testing hypotheses. For robust check of CMV, additional test carried out using the Pearson's correlation approach as suggested by Bagozzi et al. (1991). It is evident that Table 2, the correlation matrix between any of the study's variables were much less than 0.9 reaffirming no pathological threat of CMV.

## VI. Results of Hypotheses Testing

### Study One: Tests of Antecedents

The PROCESS model summary of output estimation on Hayes' (2018) of Model 14 causal inferences of the percentile of bootstrap samples of 10,000 with a 95% confidence interval. Study 1 tests the antecedents of consumers' intention to disclose personal information, which include empirical testing of perceived privacy vulnerability and perceived privacy benefits. Annex 2 presents SPSS run computations confirming H<sub>1a</sub> and H<sub>1b</sub>; thus, privacy vulnerability and privacy benefit proved to be antecedents of consumers' intention to disclose personal information. Results show that privacy vulnerability has a significant and positive effect at a regression weight of  $\beta = .098$ ,  $p < .01$ , CI [.0241 to .1728] and a model specification of  $R^2 = .136$ ,  $F(4, 330) = 13.03$ ,  $p\text{-value} = .000$  to support the predicted relationship. Similarly, privacy benefits have a statistically significant effect on consumers' intention to disclose personal information at a regression weight of  $\beta = .311$ ,  $p = .000$ , CI [.1840 to .4382] and a significant model specification of  $R^2 = .177$ ,  $F(4, 330) = 17.68$ ,  $p\text{-value} = .000$  to confirm the hypothesized relationship. Annex 3 presents SPSS run computations confirming H<sub>1d</sub> but disproving H<sub>1c</sub>. Privacy vulnerability couldn't establish an antecedental role for consumers' privacy protection behavior. Results show that privacy vulnerability hasn't had a statistically significant effect on privacy protection behavior at a regression weight of  $\beta = .017$ ,  $p > .01$ , CI [-.0399 to .0738] and a model specification of  $R^2 = .098$ ,  $F(4, 330) = 8.99$ ,  $p\text{-value} = .000$ , not to support the H<sub>1c</sub> relationship. On the contrary, privacy benefits proved to have a statistically significant effect on consumers' privacy protection behavior at a regression weight of  $\beta = -.111$ ,  $p < .05$ , CI [-.2089 to -.0119] and a significant model specification  $R^2 = .110$ ,  $F(4, 330) = 10.24$ ,  $p\text{-value} = .000$  to confirm H<sub>1d</sub>, the hypothesized relationship.

### Study Two: Tests of Mediation

We tested privacy information transparency in the mediation model. The study adapted the bootstrapping procedures for mediation test, following Zhao et al. (2010). Accordingly, we used 10,000 bootstrap samples at a 95% confidence interval (CI) as an indicator to assess mediation. Table 4 presents the results indicating privacy vulnerability has a significant effect on both privacy information transparency and consumers' intention to disclose personal information (both effects  $p < .05$ ). Moreover, privacy information transparency has a significant and positive effect on consumers' intentions to disclose personal information (effect  $p = .000$ ). Similarly, the mediation of privacy information transparency ( $\beta = -.015$  at 95% CI  $[-.036$  to  $-.001]$ ) exerts a significant indirect effect on privacy vulnerability and consumers' intention to disclose personal information. Thus, the predicted relationship (H2a) is tenable on the mediator role of privacy information transparency between the privacy vulnerability and consumers' intention to disclose personal information. Overall, the mediation result provides empirical support for the PIT's between privacy vulnerability and the intention to disclose personal information (H2a).

**Table 4: Mediation Test of H2a**

Hypothesis: H2a		(Mediator) Privacy Information Transparency (PIT)				(DV) Intention to Disclose Personal Information (IDPI)			Decision
Antecedents (IVs)	Path	Coeff.	SE	p-value	Path	Coeff.	SE	p-value	<b>Supported</b>
Constant		3.790	.125	.000		.523	.415	.209	
P. Vulnerability (Pvul)	a	-.086	.034	.012	c	.098	.038	.010	
PIT					b	.677	.105	.000	
<b>Bootstrap Indirect Effect</b>		Effect	Boot SE	LL 95% CI	UL 95% CI				
Pvul → PIT → IDPI		-.015	.009	-.036	-.001				
		R <sup>2</sup> = .019 F(1, 333) = 6.434, p-value = .012			R <sup>2</sup> = .136 F(4, 330) = 13.03, p-value = .000				

Following Judd and Kenny (1981) and Kenny et al. (1998), the causal sequential step of the mediation process, the study predicts privacy information transparency has a mediating role between privacy vulnerability and consumers' privacy protective behavior (H2b). The test was carried out using a bootstrap of 10,000 samples at a 95% confidence interval (CI). Table 5 indicates that privacy vulnerability has a negative and significant effect on the mediator (PIT). However, privacy vulnerability was found to have an insignificant effect on the dependent variable (PPB) and also on the PIT. In sum, the mediation intervening paths confirmed a negative and statistically significant effect ( $\beta = -.01$  at CI  $[-.0270$  to  $-.0004]$ , recording significant model specification at both scenarios (PIT and PPB). Thus, the study empirically concludes that perceived privacy vulnerability via privacy information transparency has a statistically significant effect on privacy protective behavior (H2b).

Table 6 presents the empirical mediation result of privacy information transparency between privacy benefits and consumers' intention to disclose personal information (H2c). Results indicate privacy benefits have both a statistically significant effect on privacy information transparency (path a =  $-.019$ ,  $p < .01$ ) and consumers' intention to disclose personal information (path c =  $.311$ ,  $p = .000$ ). Moreover, the mediator (PIT) has a significant effect on the outcome variable (IDPI) ( $b = .621$ ,  $p = .000$ ). The bootstrap indirect effect also shows a consistent result: privacy information transparency mediates between privacy benefit and consumers' intention to disclose personal information ( $\beta = -.037$ , CI  $[-.076$  to  $-.006]$ ). Hence, H2c is a tenable privacy benefit through privacy information transparency to effect consumers' intention to disclose personal information.

**Table 5: Mediation Test of H2b**

Hypothesis: H2b		(Mediator) Privacy Information Transparency (PIT)				(DV) Privacy Protective Behavior (PPB)			Decision
Antecedents (IVs)	Path	Coeff.	SE	p-value	Path	Coeff.	SE	p-value	Supported
Constant		3.79	.125	.000		3.66	.318	.000	
P. Vulnerability (Pvul)	a	-.086	.034	.012	c	.017	.029	.558	
PIT					b	-.105	.080	.188	
<b>Bootstrap Indirect Effect</b>		Effect	Boot SE	LL 95% CI		UL 95% CI			
Pvul → PIT → PPB		-.010	.007	-.0270		-.0004			
R <sup>2</sup> = .019 F(1, 333) = 6.434, p-value = .012					R <sup>2</sup> = .098 F(4, 330) = 8.99, p-value = .000				

**Table 6: Mediation Test of H2c**

Hypothesis: H2c		(Mediator) Privacy Information Transparency (PIT)				(DV) Intention to Disclose Personal Information (IDPI)			Decision
Antecedents (IVs)	Path	Coeff.	SE	p-value	Path	Coeff.	SE	p-value	Supported
Constant		4.33	.266	.000		-.333	.468	.468	
PB	a	-.19	.060	.002	c	.311	.065	.000	
PIT					b	.621	.100	.000	
<b>Bootstrap Indirect Effect</b>		Eff.	Boot SE	LL 95% CI		UL 95% CI			
PB → PIT → IDPI		-.037	.018	-.076		-.006			
R <sup>2</sup> = .029 F(1, 333) = 9.908, p-value = .002					R <sup>2</sup> = .177 F(4, 330) = 17.68, p-value = .000				

Pursuant to Judd and Kenny's (1981) and Baron and Kenny's (1986) casual steps approach to 'the mediation model' using an intervening variable, this study examined the privacy information transparency between the privacy benefit and privacy protective behavior (H2d). Table 7 shows the empirical result statistically significant on relations of privacy benefit (a = -.19, p <.01) to effect PIT and also PPB (c = -.111, p <.05). The path c connecting PIT and PPB, however, was found statistically insignificant (b = -.113, p >.05). In sum, as indicated in Table 7, the bootstrap indirect effect of PB via PIT to effect PPB has a significant effect (β = -.029, CI [-.065 to -.0038]) to support the predicted relationship H2d.

**Table 7: Mediation Test of H2d**

Hypothesis: H2d		(Mediator) Privacy Information Transparency (PIT)				(DV) Privacy Protective Behavior (PPB)			Decision
Antecedents (IVs)	Path	Coeff.	SE	p-value	Path	Coeff.	SE	p-value	Supported
Constant		4.326	.265	.000		4.195	.356	.000	
P. Benefit (PB)	a	-.190	.060	.002	c	-.111	.050	.028	
PIT					b	-.113	.078	.146	
<b>Bootstrap Indirect Effect</b>		Effect	Boot SE	LL 95% CI		UL 95% CI			
PB → PIT → PPB		-.0286	.016	-.0650		-.0038			
R <sup>2</sup> = .029 F(1, 333) = 9.91, p-value = .002					R <sup>2</sup> = .110 F(4, 330) = 10.235, p-value = .000				

**Study Three: Tests of Moderation**

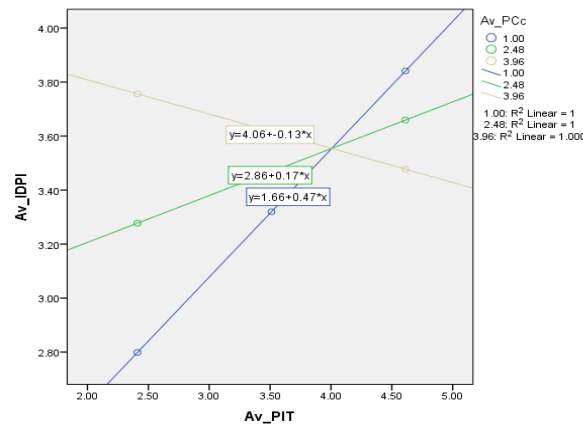
The study intends to examine two moderation hypotheses between the mediating variable, personal information transparency (PIT), and, as an outcome variable, both the intention to disclose personal information (IDPI) and the privacy protection behavior (PPB). A moderation test was run between personal information transparency (PIT) and the intention to disclose

personal information (IDPI) as moderated by privacy cynicism (PCc), denoted by H3a. Specifically, the relationship between privacy information transparency (PIT) and consumers' intention to disclose personal information will decline when there is a high influence of privacy cynicism (PCc). There was a significant main effect found between PIT and IDPI, with regression weights of  $\beta = .677$ ,  $t = 6.475$ ,  $p = .000$ , and CI [.4711 to .8823] different from zero at a 95% confidence interval of 10,000 samples. A significant interaction effect of PIT and PCc (PIT\*PCc) revealed a weight of  $\beta = .812$ ,  $t = 6.273$ ,  $p = .000$ , and CI [-.2686 to -.1386]. Besides, the indices of  $\Delta R^2 = .096$  and  $F(1,330) = 36.58$ ,  $p = .000$ , were statistically significant to test the unconditional interaction effect. Thus, the tests confirmed and supported the predicted relationships. From these results (Table 8), the study concluded that privacy information transparency and the intention to disclose personal information are moderated by privacy cynicism to support the hypothesis.

**Table 8: Analysis of Interaction Effect Hypotheses**

	Variables	$\beta$	SE	t	p	LLCI	ULCI	Decision
H3a	Intercept	.523	.415	1.259	.208	-.2939	1.3395	Supported
	PIT → IDPI	-.677	.1045	6.475	.000	.4711	.8823	
	PCc → IDPI	.812	.1295	6.273	.000	.5574	1.0667	
	PIT*PCc (Int_1)	-.203	.0335	-6.048	.000	-.2686	-.1368	
	R <sup>2</sup> Change	.0957**						
	F	36.577						
H3b	Intercept	3.661	.3178	11.52	.000	3.0360	4.2863	Supported
	PIT → PPB	-.1054	.0800	-1.318	.188	-.2628	.0519	
	PCc → PPB	-.4473	.0991	-4.514	.000	-.6423	-.2524	
	PIT*PCc (Int_2)	.112	.0257	4.358	.000	.0613	.1623	
	R <sup>2</sup> Change	.0519**						
	F	18.995						

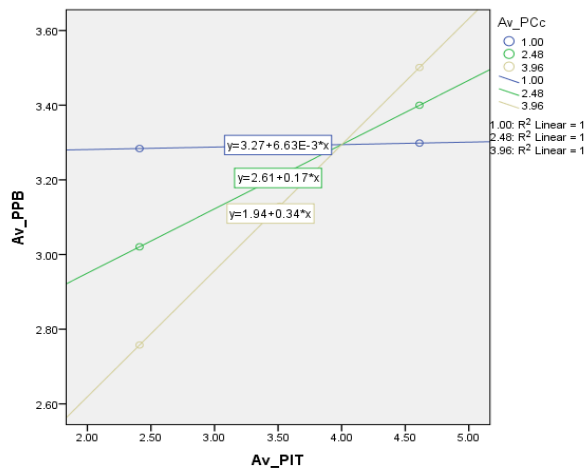
\* $p < .05$  \*\* $p = .000$



**Graph 2: Interaction Effect of H4a**

As a robust check and cross-validation, the Hayes (2018) SPSS-PROCESS macro version 3.5.3 was adopted to generate the syntax of a conditional interaction effect graph indicating low (blue), medium (green), and high (brown) levels of privacy cynicism effect in the predictor (PIT) and dependent variable (IDPI). Graph 2 depicts when PCc is perceived to have opposite slopes and a high perception of PCc in relation to its low and average perceptions. It has a statistically significant causal-effect relationship that can be concluded in congruence with the analysis made in Table 8. Hence the hypothesis denoted H3a, it can be inferred that sufficient evidence was found to support the hypothesized relationship.

The hypothesis, H<sub>3b</sub>, predicts that the impact of privacy information transparency (PIT) on consumers' perceived privacy protection will weaken when there is high privacy cynicism (PCc). The regression coefficient for the direct effect of privacy information transparency (PIT) was insignificant for respondents high at privacy protection behavior (PPB) ( $\beta = -.105, p >.05$ ) (as shown in Table 8), but the relationship between privacy cynicism (PCc) and PIT was statistically significant ( $\beta = -.447, p =.000$ ). The interaction effect (PIT\*PCc) was negative and statistically significant for respondents of high privacy cynicism ( $\beta =.112, p =.000$ ), as confirmed by the  $\Delta R^2 =.0519, F = (1,330) = 18.99$ , highly statistically significant at  $p =.000$ , CI at 95% confidence interval of 10,000 samples appeared to be non-zero [.0613 to.1623]. There is no zero between the upper and lower limits of the bootstrap result, which infers strong support for the proposed moderated model of the study.



**Figure 3: Visual aid of moderation interaction**

Validating the analysis, the SPSS syntax-generated graph, Graph 3, presents the interaction effect of privacy cynicism at low, medium, and high levels. When PCc is high, the graph shows a steeper and stronger association between PIT and PPB. Hence, H<sub>3b</sub> shows strong support for the proposed moderation relationship.

**VII. Discussions and Implications**

We systematically examined the field of privacy research in order to identify knowledge gaps about privacy risks and the behavioral responses of consumers to perceived and/or real privacy issues. Numerous studies have taught us about a variety of topics, including users' privacy behavior (Liu, 2022), privacy perceived severity, self-efficacy, and decision-making (Van Ooijen et al., 2022), the roles of privacy cynicism (Acikgoz and Vega, 2022), and determining the effects of privacy information transparency (Agozie and Kaya, 2021). This study intends to clarify the causes of both outcome variables (consumers' intention to share personal information and privacy protective behavior), depending on the call for research. We also investigated the impact of privacy information transparency on both the independent factors (privacy vulnerability and benefits) and the outcome variables. Additionally, it investigated the moderating functions of privacy cynicism in relation to the outcome variables and the mediating variable (privacy information transparency). Specifically, we use the intricate model of direct, mediating, and moderating links to offer insights into privacy science. Study 1 added to the body of literature by demonstrating the importance of three of the four hypothesized relationships between customers' desire to disclose personal information and their privacy-protective behavior. Coherent to our findings, Walter and Abendroth (2020), e-platforms' useful benefits have a direct influence on people's development of a favorable

attitude toward them, Kim et al. (2019), providing customers with the ability to limit who can access their personal data is a crucial component of privacy management and control.

The four proposed associations were validated when we looked at the mediation of privacy information transparency between the independent factors and outcome variables. According to research that has been published, a person's perceived vulnerability indicates their sensitivity to threats; those who regard themselves as more vulnerable are more aware of the need for information system security protection (Hameed & Arachchilage, 2019). Additionally, the paper adds value by clarifying how the regression between privacy information transparency and both outcome variables are influenced by a larger degree of privacy cynicism. This pertains to the concept of mistrust issues, which may serve as a springboard for cynicism that could lead to a loss of trust in the system of an organization (Bateman et al., 1992), and more especially, in the study's setting of online platform design, implementation, and assessment. Overall, nine out of the 10 expected correlations are supported empirically by Table 9.

**Table 9: Overview of Hypotheses Testing**

Hypo.	Relationships	Decision	Conclusion
H1a	Pvul → IDPI (+)	Supported	Perceived privacy vulnerability positively affects consumers' intention to disclose personal information.
H1b	PB → IDPI (+)	Supported	Perceived privacy benefit is a positive antecedent of consumers' intention to disclose personal information.
H1c	Pvul → PPB (+)	Not Supported	Perceived privacy vulnerability unable to contribute to become as an antecedent of consumers' privacy protection behavior.
H1d	PB → PPB (-)	Supported	Perceived privacy benefit is a negative antecedent of consumers' privacy protection behavior.
H2a	Pvul → PIT → IDPI (-)	Supported	Perceived privacy information transparency mediates the effect of privacy vulnerability on consumers' intention to disclose personal information.
H2b	Pvul → PIT → PPB (-)	Supported	Perceived privacy information transparency mediates the effect of privacy vulnerability on consumers' privacy protection behavior.
H2c	PB → PIT → IDPI (-)	Supported	Perceived privacy information transparency mediates the effect of privacy benefit on consumers' intention to disclose personal information.
H2d	PB → PIT → PPB (-)	Supported	Perceived privacy information transparency mediates the effect of privacy benefit on consumers' privacy protection behavior.
H3a	Int_1 PIT*PCc (-)	Supported	Higher privacy cynicism significantly and negatively affects the interaction between privacy information transparency and consumers' intention to disclose personal information.
H3b	Int_2 PIT*PCc (+)	Supported	Higher privacy cynicism significantly affects the interaction between privacy information transparency and consumers' intention to disclose personal information.

*N.B.* Pvul = Privacy Vulnerability, PB = Privacy Benefits, PIT = Privacy information transparency, PCc = Privacy Cynicism, IDPI = Consumers' intention to disclose personal information and PPB = privacy protection behavior.

**Theoretical Implications**

Multiple theoretical advances are made by the research to the corpus of current knowledge. The first factor influencing consumers' decision to divulge personal information is privacy vulnerability. Although Dunbar et al. (2021) suggested broadening our focus on privacy requirements and vulnerabilities, there hasn't been much research done on the topic, especially when it comes to online platforms. Here, we developed measures of vulnerability, looked at the intentions to disclose personal information, and applied notions of privacy vulnerability to scenarios involving users of online platforms. As a result, we hope that our study will act as a starting point and a point of reference for researchers looking into privacy vulnerability and related issues. Second, it offers new perspectives on privacy advantages as a predicate of customers' intention to disclose personal data and their privacy-protecting



actions. This is consistent with filling in the research gaps on privacy behavior and the cost-benefit analysis of privacy (Van Ooijen et al., 2022) by implementing generalizability methodologies (Liu, 2022). We used a systematic random sample strategy to validate and add to the privacy literature while keeping in mind generalizability. Furthermore, it has been suggested that the benefits of privacy have a direct bearing on customers' intentions to disclose personal information as well as their actions to preserve their privacy when using online platforms. Furthermore, it sheds light on how consumers' perceptions of the benefits of privacy greatly influence both privacy protection behavior and consumers' intention to disclose personal information that the current controversy surrounding the "privacy paradox" (Tang et al., 2020). Thirdly, the study emphasized how privacy information openness influences users of online platforms' privacy vulnerability and benefits, influencing their plans to reveal personal information as well as their actions to protect it. It is anticipated to address current research gaps and ambivalence around privacy information openness (see, for example, Agozie & Kaye, 2021). The outcome emphasizes how important privacy information openness is in mediating the relationship between consumers' intention to disclose personal information (privacy protective behavior) and privacy vulnerability (benefits). Finally, we looked at the connection between consumers' intention to share personal information (privacy protective behavior) and privacy pessimism regarding transparency of privacy information. Notably, it broadens our understanding of the moderating influence of privacy cynicism, in line with the research requests made by Acikgoz and Vega (2022) and Dunbar et al. (2021). The results of the study, which add to the body of knowledge on privacy, demonstrated how consumers' increased sense of privacy cynicism affects online platform users' intentions to reveal personal information and the transparency of privacy information.

### ***Practical Implications***

The current study provides several policy implications for online platform designers, marketers, and CEOs. First, keep in mind that online platforms have created several value-adding elements for consumers' wellbeing and, at the same time, raised extensive privacy risks. Maslach et al. (2001) emphasized the need to deploy a serious, strict policy on privacy protection. Without handling privacy information with due care, it can plunge the already-built goodwill and cause irreversible damage on online platforms. Therefore, providers of online platforms should consider the critical role of consumers' perceived privacy vulnerability in impacting their intention to disclose personal information, and, on the other hand, perceived privacy benefits influence both privacy protection behavior and the intention to disclose personal information. Thus, online platforms are expected to be vigilant about operations, review current gaps and perceptions, and adjust systems in managing decisions to protect consumers' personal information. Second, the CEO's and marketing officers of online platforms need to pay attention to consumers' perceptions and actual experiences of privacy risks. The study confirmed the intervening role of privacy information transparency between privacy vulnerability (benefits) and consumers' intention to disclose personal information (privacy protection behavior). Measures are required to counter an unintended privacy disclosure, starting with online platform design, implementation, review, and adjusting to control the entire ins and outs of consumers' privacy information. Additionally, privacy cynicism can be caused by ill-defined online platform policies or their execution. Collecting consumers' personal data and leaking it to unauthorized intruders would raise privacy cynicism in consumers' minds. Therefore, providers of online platforms should try to identify the root causes of perceived privacy cynicism and conduct evidence-based promotion, system changes, and continuous evaluation to clear up privacy cynicism or to relieve consumers' privacy issues. Practitioners also assess consumers' characteristics and individual requirements for privacy management to gradually develop user-friendly online platforms.

### **Limitations of the study**

Despite this study's merits, there are a number of drawbacks that provide room for more investigation. Firstly, the researchers employed a cross-sectional approach, which implies gathering all of the survey data at once. Given the potential issues of generalizability, we recommend incorporating other study designs, such as experimental studies, or the case approach for additional research validation. Secondly, while the sample size is appropriate, future research should increase it to achieve the desired size. Third, a more thorough examination of the role that consumer demographics like age, sex, wealth, and educational attainment play in moderating the relationship between privacy factors would be intriguing. Fourth, longitudinal studies could also be particularly illuminating for privacy research in such frameworks to determine whether they fit with this conclusion or not (Lee et al., 2022). Some people could advocate for a robust longitudinal research strategy that could test the theoretical and managerial implications. Furthermore, researchers in the field could gain insights from comparable analyses of cross-sectional and longitudinal approaches in privacy-related research.

### **Conclusions**

The purpose of this study is to examine the antecedents of consumers' intention to disclose personal information and privacy protection behavior on online platforms, discover the intervening roles of privacy information transparency, and explore the moderation roles of privacy cynicism. Three out of four hypotheses related to antecedents of consumers' intention to disclose personal information and privacy protection behavior have been confirmed to build on privacy literature and back up online platform operators. As predicted by the research model, the entire mediation of privacy information transparency has been proven to add value to the existing body of knowledge and provide practical guidelines for practitioners. Furthermore, this study confirmed the impact of privacy cynicism on the intricate research model, highlighting its significance in the privacy literature and offering guidance to online platform policy designers, marketers, and CEOs.

### **References**

- Acikgoz, F. & Vega, R. P. (2022). The Role of Privacy Cynicism in Consumer Habits with Voice Assistants: A Technology Acceptance Model Perspective, *International Journal of Human-Computer Interaction*, 38:12, 1138-1152, DOI: 10.1080/10447318.2021.1987677.
- Agozie D., Nat M. (2020). Investigating the Antecedents and Role of Usage Fatigue on Online Commerce Usage Decrease. *International Journal of E-Business Research*, 16(4), DOI: 10.4018/IJEER.2020100101.
- Agozie, D.Q.; Kaya, T. (2021). Discerning the effect of privacy information transparency on privacy fatigue in e-government. *Gov. Inf. Q.* 38, 101601.
- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34-49.
- Alzaidi, M. S. & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services* 68, 103042, <https://doi.org/10.1016/j.jretconser.2022.103042>.
- Andersson, U., Cuervo-Cazurra, A., & Nielsen, B. B. (2020). Explaining interaction effects within and across levels of analysis. In L. Eden, B. Nielsen, & A. Verbeke (Eds.), *Research methods in international business* (pp. 331-349).
- Ballantyne, C. (2005). Moving student evaluation of teaching online: reporting pilot outcomes and issues with a focus on how to increase the student response rate. Paper presented at the 2005 Australasian Evaluations Forum: University Learning and Reaching: Evaluating and Enhancing the Experience, UNSW, Sydney.

- Baron, R., & Kenny, D. (1986). The Moderator Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Consideration *Journal of Personality and Social Psychology*, 1 (51) 1173-82.
- Bateman, T. S., Sakano, T., & Fujita, M. (1992). Roger, me, and my attitude: Film propaganda and cynicism toward corporate leadership. *Journal of Applied Psychology*, 77(5), 768–771.
- Beavers, A. S. Lounsbury, J. W. Richards, J. K. Huck, S. W. Skolits, G. J. and Esquivel, S. L. (2013). Practical considerations for using exploratory factor analysis in educational research, *Pract. Assess. Res. Eval.* 18, 1 (2013).
- Bagozzi, R., Yi, Y., & Phillips, L. (1991). Assessing Construct Validity in Organizational Research. *Administrative Science Quarterly*, 36(3), 421–458.
- Boush, D. M., Kim, C. H., Kahle, L. R., & Batra, R. (1993). Cynicism and conformity as correlates of trust in product information sources. *Journal of Current Issues & Research in Advertising*, 15(2), 71–79.
- Brown, T. A. (2015). *Confirmatory Factor Analysis for Applied Research*, 2nd ed. (Guilford Publications, New York, NY).
- Burke, R. R. (1997). Do you see what I see? The future of virtual shopping. *Journal of the Academy of Marketing Science*, 25(4), 352–360.
- Chang, S.J. and Eden, W.L. (2010). From the editors: common method variance in international business research. *Journal of International Business Studies*, Vol. 41 No. 2, pp. 178-184.
- Chaouali, W., Souiden, N., & Ladhari, R. (2017). Explaining adoption of mobile banking with the theory of trying, general self-confidence, and cynicism. *Journal of Retailing and Consumer Services*, 35, 57–67.
- Chin (2023). Top 23 Biggest Data Breaches in US History <https://www.upguard.com/blog/biggest-data-breaches-us>.
- Cho, Y.K., Sutton, C.L., (2021). Reputable internet retailers' service quality and social media use. *Int. J. Electron. Commer. Stud.* 12 (1), 43–64
- Choi, H.; Park, J.; Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Comput. Hum. Behav.* 81, 42–51.
- Choi, S., Mattila, A. Bolton, L. (2020). To Err Is Human (-oid): How Do Consumers React to Robot Service Failure and Recovery? *Journal of Service Research* 1-18, [sagepub.com/journals-permissions](https://www.sagepub.com/journals-permissions) DOI: 10.1177/1094670520978798
- Couper, M. (2000). Web surveys: A review of issues and approaches. *Public Opinion Quarterly*, 64, 464-494.
- Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, 79(2), 73–91.
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease OF Use, and User Acceptance OF Information Technology. *Mis Quarterly* (13:3) 319-339.
- Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, 38(3), 475–487.
- De Wolf, R. (2020). Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media Soc.* 2020, 22, 1058–1075.
- Dean, J. J., Brandes, W., & Dharwadkar, R. (1998). Organizational cynicism. *Academy of Management Review*, 23(2), 341–352.
- Dillman D. A., Smyth J. D., Christian L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method*. Hoboken, NJ: John Wiley & Sons, Inc.
- Dillman, D.A. (2007). *Mail and Internet Surveys: The Tailored Design Method (2007 update with new Internet, visual, and mixed-mode guide)*, 2nd ed. New York: John Wiley.
- Dinev, T., Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behav. Inform. Tech.* 23(6) 413–422.
- Dinev, T., Hart, P., (2006). An extended privacy calculus model for e-commerce transactions. *Inform. Syst. Res.* 17 (1), 61–80.
- Dunbar, J.C.; Bascom, E.; Boone, A.; Hiniker, A. (2021). Is Someone Listening? Audio-Related Privacy Perceptions and Design Recommendations from Guardians, Pragmatists, and Cynics. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 5, 1–23.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with un- observable variables and measurement error. *Journal of Marketing Research*, 18(1) 39-50.

- Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behavior: Towards an integrated model. *European Research on Management and Business Economics*, 22(3), 167–176.
- Ghauri, P., & Gronhaug, K. (2010). *Research Methods in Business Studies: A Practical Guide*. (Fourth Edition ed.) FT-Pearson.
- Goldfarb, A., & Tucker, C. (2011). Online display advertising: Targeting and obtrusiveness. *Marketing Science*, 30(3), 389–404.
- Hameed, M. H., Arachchilage, N. A. (2019). On the Impact of Perceived Vulnerability in the Adoption of Information Systems Security Innovations. *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.11 (4) 9-18. DOI: 10.5815/ijcnis.2019.04.02.
- Hanus, B. & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, 33 (1) 2-16.
- Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). New York, NY: Guilford Press.
- Ibrahim, M. A., & Narczyk, R. (2015). Adoption of ERP systems: Does information transparency matter? *Telematics and Informatics*, 32(2), 300–310.
- Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers and Security*, vol. 31, pp. 83-95.
- Jin, L. (2022). Review of Research on the Privacy Protection Behavior of Social Network Users. *Advances in Social Science, Education and Humanities Research*, volume 631, Proceedings of the 2021 International Conference on Social Development and Media Communication (SDMC 2021).
- Judd, C. M., & Kenny, D. A. (1981). *Estimating the effects of social interventions*. Cambridge, England: Cambridge University Press.
- Kaiser, H. F. (1974). An index of factorial simplicity, *Psychometrika* 39, 31.
- Kenny, D. A., Kashy, D. A., & Bolger, N. (1998). Data analysis in social psychology. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (pp. 233–265). Boston: McGraw-Hill.
- Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273–281.
- Kim, H. W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: An empirical investigation. *Decision Support Systems*, 43(1), 111–126.
- Kotler, P. & Armstrong, G. (2015). *Principles of Marketing*. Pearson.
- LaRose, R. & Rifon, N. J. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, 41 (Summer): 127–149.
- Lee, C.B.; Io, H.N.; Tang, H. (2022). Sentiments and perceptions after a privacy breach incident. *Cogent Bus. Manag.* 9, 2050018.
- Lee, Y., & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executive's Decision to Adopt Anti-malware Software. *European Journal of Information Systems*, 18, (2) 177-187.
- Liu B., (2022). Study on the influence mechanism of user's information privacy behavior from the perspectives of both technical characteristics and individual difference, *Journal of Modern Information*, <https://kns.cnki.net/kcms/detail//22.1182.G3.20221202.1535.002.html>.
- Luo, N.; Wang, Y.; Zhang, M.; Niu, T.; Tu, J. (2020). Integrating community and e-commerce to build a trusted online second-hand platform: Based on the perspective of social capital. *Technol. Forecast. Soc. Chang.* 153, 119913.
- Lutz, C.; Hoffmann, C.P.; Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media Soc.* 22, 1168–1187.
- Lwin, M., Wirtz, J., & Williams, J. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(1), 572–585.
- Malhotra, N. K. (2004). Common method variance in Information Systems Research: A comparison of alternative approaches and analysis of past research, *Journal on management science*, 8(1).
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155.

- Maslach, C., Schaufeli, W.B. and Leiter, M.P. (2001), "Job burnout", *Annual Review of Psychology*, Vol. 52 No. 1, pp. 397-422.
- Mendenhall, M. E., Black, J. S., Jensen, R. J., & Gregersen, H. B. (2003). Seeing the elephant: Human resource management challenges in the age of globalization. *Organizational Dynamics*, 32(3), 261-274.
- Meso, P. Ding, Y. and Xu, S. (2013). Applying Protection Motivation Theory to Information Security Training for College Students. *Journal of Information Privacy and Security*, 9, (1) 47-67.
- Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26(4), 323-339.
- Moriuchi, E. (2019). Okay, Google! An empirical study on voice assistants on consumer engagement and loyalty. *Psychology & Marketing*, 36(5), 489-501.
- Ng, B. Y. Kankanhalli, A. and Xu, Y. (2009). Studying Users' Computer Security Behavior Using the Health Belief Model. *Decision Support Systems*, 46 (4) 815- 825.
- Norberg, Patricia A., Daniel R. Horne, and David A. Horne. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41 (Summer): 100-126.
- Ofori, K. S., Larbi-Siaw, O., Fianu, E., Gladjah, R. E., & Boateng, E. O. Y. (2016). Factors influencing the continuance use of mobile social media: The effect of privacy concerns. *Journal of Cyber Security and Mobility*, 4(3), 105-124.
- Park Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, 38, 296 - 303.
- Park, Y., & Chen, J. V. (2007). Acceptance and adoption of the innovative use of smartphone. *Industrial Management & Data Systems*, 107(9), 1349-1365.
- Petronio S (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.
- Petronio S., & Durham, W. (2015). *Communication privacy management theory. Significance for interpersonal communication*, Sage publication.
- Podsakoff, P.M., Mackenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903.
- Quach, S., Thaichon, P., Martin, K., Weaven, S., Palmatier, R. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, available <https://doi.org/10.1007/s11747-022-00845-y>.
- Regoli, R. M. (1976). The effects of college education on the maintenance of police cynicism. *Journal of Police Science and Administration*, 4(3), 340-345.
- Saunders, C. (2014). Anti-Politics in Action? Measurement Dilemmas in the Study of Unconventional Political Participation. *Political Research Quarterly* 67(3):574-88.
- Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students*. Pearson Education Ltd., Harlow.
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. 5th ed., Pearson Education Limited.
- Sen, R. and Borle, S. (2015). Estimating the contextual risk of data breach: an empirical approach. *Journal of Management Information Systems*, 32 (2) 314-341.
- Stanton, J., Stam, K., Mastrangelo, P. & Jolton, J. (2005). Analysis of End User Security Behaviors, *Computers and Security*, 24 (2) 124-133.
- Sutanto, J., Palme, E., Chuan-Hoo, T., & Phang, C. W. (2013). Addressing the personalization- Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *Management Information Systems Quarterly*, 37(4), 1141-1164. doi:10.25300/MISQ/2013/37.4.07.
- Tang, J.; Akram, U.; Shi, W. (2020). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *J. Enterp. Inf. Manag.* 34, 1097-1120.
- Thompson, R. C., Joseph, K. M., Bailey, L. L., Worley, J. A., & Williams, C. A. (1999). *Organizational change: An assessment of trust and cynicism*. US Department of Transportation: Federal Aviation Administration.
- Tu, C. Z., Adkins, J. & Zhao, G. Y. (2018). Complying with BYOD Security Policies: A Moderation Model. In the Proceedings of the Midwest Association for Information System (MWAIS).

Utz, S. (2015). The function of self-disclosure on social network sites: Not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. *Computers in Human Behavior*, 45,1-10.

van Ooijen, I.; Segijn, C.M.; Oprea, S.J. (2022). Privacy Cynicism and its Role in Privacy Decision-Making. *Commun. Res.* 1-32.

Walgrave, S., and J. Verhulst. (2011). Selection and Response Bias in Protest Surveys. *Mobilization: An International Quarterly* 16(2):203-22. <https://doi.org/10.17813/maiq.16.2.j475m8627u4u8177>.

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing*, 35(1) 144-158.

Walter, J., & Abendroth, B. (2020). On the role of informational privacy in connected vehicles: A privacy-aware acceptance model- ling approach for connected vehicular services. *Telematics and Informatics*, 49, 101361J. <https://doi.org/10.1016/j.tele.2020.101361>.

Watanabe, N.M., Kim, J., Park, J., (2021). Social network analysis and domestic and international retailers: an investigation of social media networks of cosmetic brands. *J. Retailing Consum. Serv.* 58 (4), 102301.

Welman, C., Kruger, F., & Mitchell, B. (2005). *Research Methodology*. (3rd ed.) Oxford University Press.

Wottrich, V. M., Reijmersdal, E. A., & Smit, E. G. (2019). App users unwittingly in the spot- light: A model of privacy protection in mobile apps. *Journal of Consumer Affairs*, 53(3), 1056-1083.

Xu, J. D., Benbasat, I., & Cenfetelli, R. (2011). The effects of service and consumer product knowledge on online customer loyalty. *Journal of the Association for Information Systems*, 12 (11), 741-766.

Xu, J., Benbasat, I., & Cenfetelli, R. T. (2014). The nature and consequences of trade-off transparency in the context of recommendation agents. *MIS Q.*, 38(2), 379-406.

Yang, H., & Lee, H. (2019). Understanding user behavior of virtual personal assistant devices. *Information Systems and e-Business Management*, 17 (1), 65-87.

Yin, R.K. (2003). *Case Study Research: Design and Methods*. 3rd Edition, Sage, Thousand Oaks.

Zeng, F., Chi, Y., & Dong, M. C. (2020). Effects of Reward on Observers in a Distribution Network. *Industrial Marketing Management* in press.

Zhao, Xinshu, John G. Lynch, and Qimei Chen (2010). Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. *Journal of Consumer Research*, 37 (2), 197-206.

Zhou, L., Weiquan, W. J., Xu, D., Liu, T., & Gu, J. (2018). Perceived information transparency in B2C e-commerce: An empirical investigation. *Information & Management*, 55(7), 47-79.

**Annex-1 Standard Regression Weights, CR, AVE, Communalities, and Cronbach’s α**

Paths	Standardized Reg. Estimate	CR	AVE	Cronbach’s α	Communalities Extraction		
PV1	<---	Pvul	0.956	0.984	0.926	0.984	.929
PV2	<---	Pvul	0.939				.909
PV3	<---	Pvul	0.953				.925
PV4	<---	Pvul	0.975				.952
PV5	<---	Pvul	0.987				.967
PB1	<---	Pben	0.498	0.850	0.668	0.779	.650
PB2	<---	Pben	0.918				.888
PB3	<---	Pben	0.956				.904
PCc1	<---	Pcyn	0.918	0.924	0.802	0.847	.881
PCc2	<---	Pcyn	0.931				.885
PCc3	<---	Pcyn	0.834				.815
PIT1	<---	Pinf	0.565	0.851	0.595	0.932	.516
PIT2	<---	Pinf	0.770				.716
PIT3	<---	Pinf	0.909				.801
PIT4	<---	Pinf	0.801				.727
IDPI1	<---	Idis	0.803	0.935	0.828	0.931	.815
IDPI2	<---	Idis	0.960				.906
IDPI3	<---	Idis	0.958				.913
PPB1	<---	Ppro	0.632	0.853	0.599	0.772	.834
PPB2	<---	Ppro	0.223				.652

PPB3	<---	Ppro	0.635				.850
PPB4	<---	Ppro	0.916				.812
PPB5	<---	Ppro	0.868				.810
PPB6	<---	Ppro	0.748				.763

**Annex-2: Model Coefficients for Antecedents of Intention to Disclose Personal Information**

Antecedents	Paths	Consumers' Intention to Disclose Personal Information (DV)						Results
		Coeff	SE	t	p	LLCI	ULCI	
Constant		.523	0.415	1.259	.208	-.2939	1.3395	
Av_Pvul	H <sub>1a</sub>	.098	0.038	2.606	0.001	.0241	.1728	Supported
Constant		-.333	.458	-.727	.467	-1.234	.568	
Av_PB	H <sub>1b</sub>	.311	0.065	4.816	.000	.1840	.4382	Supported
Model Specification		H <sub>1a</sub> : R <sup>2</sup> = .136 F(4, 330) = 13.03 p-value = .000			H <sub>1b</sub> : R <sup>2</sup> = .177 F(4, 330) = 17.68 p-value = .000			

**Annex-3: Model Coefficients for Antecedents of Consumers' Privacy Protection Behavior**

Antecedents	Paths	Consumers' Privacy Protection Behavior (DV)						Results
		Coeff	SE	t	p	LLCI	ULCI	
Constant		3.66	.318	11.521	.000	3.036	4.287	
Av_Pvul	H <sub>1c</sub>	.017	.029	.586	.558	-.0399	.0738	Not Supported
Constant		4.195	.357	11.768	.000	3.4938	4.8965	
Av_PB	H <sub>1d</sub>	-.111	.050	-2.2032	.028	-.2098	-.0119	Supported
Model Specification		H <sub>1c</sub> : R <sup>2</sup> = .098 F(4, 330) = 8.99 p-value = .000			H <sub>1d</sub> : R <sup>2</sup> = .110 F(4, 330) = 10.24 p-value = .000			

**Cite this article:**

**Sefora Hailu Yoseph & Gao Chongyan** (2024). Antecedents of Consumers' Privacy Protection Behavior and Intention to Disclose Personal Information: Mediating Role of Personal Information Transparency. *International Journal of Science and Business*, 37(1), 96-118. DOI: <https://doi.org/10.58970/IJSB.2388>

Retrieved from <http://ijsab.com/wp-content/uploads/2388.pdf>

**Published by**

