

The Disparity Effects of Privacy Turbulence, Control, and Information Transparency on the Intention to Disclose Personal Information: The Moderating Role of Privacy Cynicism

Sefora Hailu Yoseph¹ & Gao Chongyan²

Abstract

This study examined privacy issues in online platforms that encompass a complex research model of direct, indirect, and interaction effects using the (Hayes A. F., 2018) PROCESS model 58. A systematic stratified clustered sample of 335 consumers participated in the study. The analysis showed privacy turbulence was a strong antecedent of consumers' intention to disclose personal information. Against our prediction, privacy control couldn't be empirically supported to become an antecedent of the intention to disclose personal information. The mediation role of personal information transparency between privacy turbulence and the intention to disclose personal information revealed significant evidence to support the hypothesis. The entire moderation tests of privacy cynicism appeared to be statistically significant in line with our predicted relationships. The study portrayed theoretical and managerial implications that accompanied with some limitations that could be a basis to undertake future research.

Keywords

Privacy turbulence Privacy control Personal information transparency Privacy Cynicism Intention to disclose personal information

Date of Submission: 20-09-2024

Date of acceptance: 05-10-2024

I. Background

With the advent of the internet, consumers tend to enjoy online services that greatly improve their livelihood and services catered from anywhere. Equally, consumers tend to feel somehow invaded privacy since digitalized personal profiles are transferred or intruders may use those data without the permission and consent of an individual. With continued privacy breaches and turbulences, consumers expect concrete measures on safeguarding their privacy data to build confidence in online services. Consumers used to interact with online platforms or utilize services when they built trust (Abdelmoety et al., 2022) as opposed to the high prevalence of privacy invasions. On the other hand, online service providers have greater opportunities to provide tailored services to individual consumers' needs owing to a database of personalized information. As requirements for online services, consumers are expected to improve transparency and accessibility of their privacy information (Ginder and Byun, 2022) to a particular platform that is believed and experienced to have a privacy control system.

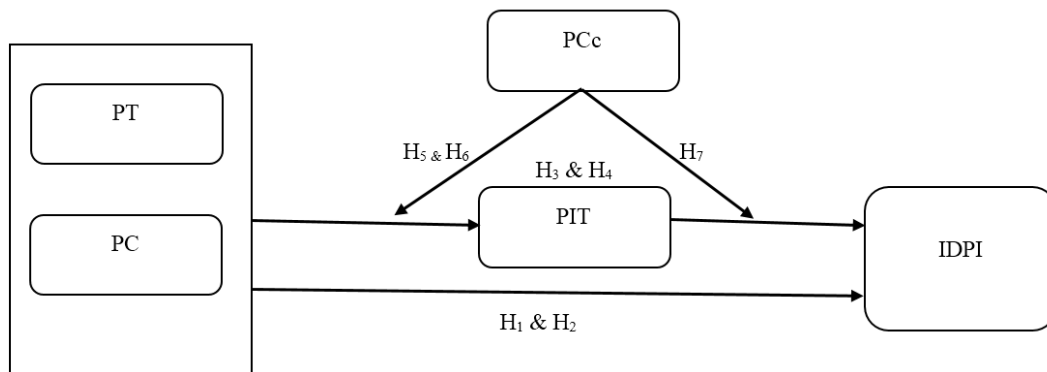
Consumers are tempted to resist on using online platforms because of periodic data breaches, insecurity, and incomplete privacy control that could be a basis for their privacy cynicism. Consumers' privacy-related decisions (Weisburd, 2019; Razi et al., 2020) has been observed to cause significant dilemma, and conflict to adopt in online behavior. In line with the research needs on capturing changes and new development in online service environment (Agozie et al., 2022), this study intends to exploring the disparities of privacy turbulence, control, and information transparency effects on consumers' intention to disclose personal information.

Keeping consumer's privacy in control is a high level of responsibilities, challenging, and a project with no-end that cannot be scaled (Solove, 2021). Although service providers attempt to make privacy regulations that frequently aim at alleviating privacy protection, several consumers' experience witnessed that excessively affect their lives due to intrusions, undeclared ads, data theft, and privacy turbulences. Once the data is in the hands of service platforms, it is beyond consumer's control and their personal data may fall short of its intended purposes. Despite the fact that several ground-breaking studies have looked at online privacy in general (e.g., Martin et al.,

¹ Contact: Sefora Hailu, hailusefora@gmail.com, Business School, International Marketing – University of International Business and Economics (UIBE), Beijing, 100029, PRC.

² Associate Professor, gaochongyan1@qq.com Business School, International Marketing – University of International Business and Economics (UIBE), Beijing, 100029, PRC

2017; Mousavizadeh et al., 2016; Gong et al., 2019), there have been relatively few systematic attempts to provide a theoretical framework on multiple factors that include intervening and interacting variables. Thus, this research aims to address a number of research calls. 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 attempt to address the call for research on consumers' 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 information transparency (Agozie & Nat, 2020; Choi, 2020; Kim et al., 2019; Alzaidi & Agag, 2022; Jin, 2022). In view of this background, we conceptualize the disparity effects of privacy turbulence, control, and information transparency on the intention to disclose personal information: the moderating role of privacy cynicism. The proposed conceptual framework can be represented as follows:



Note: PT = perceived privacy turbulence, PC = perceived privacy control, PCc = perceived privacy cynicism, PIT = privacy information transparency, and IDPI = intention to disclose personal information

Theoretical Framework and Hypotheses Development

Intention to Disclose Personal Information

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. Compared with customers who do not disclose and are unexpectedly presented with personalized promotions, customers who participate in self-disclosure are more likely to engage with personalized promotions designed on the basis of analytics of such data because of their need for consistency (Zeng et al., 2020). Additionally, 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 induces 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.

Although consumers' data can be gathered by businesses from a variety of sources, a substantial amount of extremely sensitive information can be obtained through customer self-disclosure. In this context, self-disclosure is an active gesture that indicates consent given to businesses for access to client information (Martin et al., 2017). Businesses have the right to request personal information from clients who are registering online for the first time in regards to the practice of self-disclosure (Zeng et al., 2020). Companies also periodically remind customers to update their important information throughout subsequent transactions. In this way, the choice of what data to collect and whether to reveal is shifted from the company to the clients themselves. According to Zeng et al. (2020), research on self-disclosure has been done in two different ways. The first stream concentrated on the relationship between self-disclosure and intimacy and trust (Moon, 2000), while the second stream primarily looked at how interviewee traits affected their intents to disclose (Utz, 2015). There are still unsolved questions about the effects of self-disclosure on customer purchases, its causes, and the important privacy policies that encourage it.

Studies indicated using a compliance-promoting heuristic in the intervention setting to attain self-disclosure compliance at the initial stage (Fennis et al., 2009; Khan et al., 2011). Among the most crucial tactics used by businesses to gather personal data while allaying consumers' privacy fears and boosting their willingness to divulge personal information are privacy assurance and personalization declaration (Hui et al., 2007). In order to increase compliance at the first self-disclosure stage, personalization declarations imply future benefits that businesses can provide to customers (such as convenient purchasing experiences and tailored products or services). In particular, companies can create greater feelings of empowerment in their customers if they offer them both privacy assurance and a personalization declaration in the context of the intervention. This will help them avoid risks and gain personalized benefits, which will increase their commitment during the initial stage of self-disclosure (both the act of self-disclosure and the intensity of self-disclosure). By elucidating the firms' obligation to guarantee the security of their data, privacy assurance empowers customers' perceived control over security risks and aids in their more accurate assessment of the privacy risks associated with disclosing personal information to them (Hui et al., 2007; Bao & Ni, 2017). Two approaches to self-disclosure research have been taken, according to Zeng et al. (2020). The first stream focused on the connection between intimacy, trust, and self-disclosure (Moon, 2000), whereas the second stream mainly examined the ways in which respondent qualities influenced their disclosure intentions (Utz, 2015). Unanswered concerns remain regarding the reasons behind self-disclosure, how it affects consumer loyalty to online platforms, and the crucial privacy laws that support it.

Privacy Turbulence

Privacy turbulence occurs due to the breakdown in privacy regulation and management implying disruptions on privacy ownership, control, limits, norms, and boundaries (Petronio & Child, 2020). It is the degree and type of disturbances that take place as recurring problems the conditions for privacy instability. Uncertainty over privacy might vary from small problems to complete collapses. The online platform landscape is open and dynamic, prone to context collapses (Vitak, 2012) and invisible audiences (Litt, 2012), making breakdowns or turbulences a common occurrence. Online platform turbulence can happen in a variety of ways, with various relationship ramifications that follow. For instance, a variety of factors might lead to modifications in the blogging privacy policies that individuals employ (Child et al., 2011). According to research by DeGroot and Vik (2017), privacy turbulence was likely to result from the absence of clear privacy regulations; after encountering privacy problems, prior study has discovered behaviors of updating, adjusting, and correcting privacy regulations (Child and Starcher, 2017; Child et al., 2011).

Manage impressions more skillfully to better safeguard personal identity and safety was the main motivation behind people adjusting their privacy policies to better protect private information (Petronio & Child, 2020). There was also an identification of the need to avoid legal or disciplinary issues as well as to placate significant relationship partners (Child et al., 2012); further investigation discovered that individuals consistently employed a variety of content removal techniques to appropriately protect their privacy whenever they were more transparent and porous with their present privacy policies (Child et al., 2011). Accordingly, consumers actively control their privacy and pay attention to what they disclose on online platform in order to avoid more breakdowns.

Alternatively, turbulence in private information is a reflection of the times when people's privacy management fails. Unrest is normal and can range from major incidents such as unauthorized spying to smaller transgressions (e.g., Petronio, 2002). Creating shared privacy boundaries, coordinating privacy borders, and managing the effects of privacy turbulence are just a few of the ways in the process of managing private information (Petronio & Durham, 2008). The repercussions become more troublesome if privacy turbulence happens within a valued interpersonal relationship because the initial owner's presumed degree of confidence is likely to be viewed as misplaced. It goes without saying that the conditions causing the turbulence or breakdowns might have a wide variety of effects. Additionally, the recipient can face confidentiality issues. Even more terrible circumstances in which consenting co-owners receive an explicit privacy rule instructing them not to divulge the original owner's information to a specific person, but they nevertheless do so, severely harming their relationship (Petronio & Bantz, 1991). Hence, this study proposes that privacy turbulences directly affects consumers' intention to disclose personal information in interacting with online platforms.

H₁: Consumers' perceived privacy turbulences (PT) negatively affect their intention to disclose personal information (IDPI).

Privacy Control

The concept of privacy has been the subject of intense discussion in recent years, with the major points of contention being the significance of sophisticated technologies and the increased potential for privacy infringement (Lee et al., 2017). The right of consumers to controllability has been highlighted in numerous research as a privacy principle (Rossle, 2004). For instance, Bellman et al., (2004) characterize privacy worries as fear of an external intrusion on one's private over which the user has no control, and Stone et al. (1983) define privacy control as the capacity to regulate public access to personal information. Accordingly, Kim et al. (2019) note that a key component of privacy management must be giving consumers the ability to limit who can access

their personal data. Furthermore (Lee Y. &, Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. , (2009))re, click rates for tailored web advertisements are impacted by consumers' perceptions of control over their personal information. According to earlier research, individuals rarely care about tailored advertisements and divulge more details when adjusting their control settings (Tucker, 2014; Brandimarte et al., 2013). Tucker (2014), for instance, found that users clicked on tailored advertising twice as frequently following the announcement of improved privacy control features. Additionally, Xu (2007) proposed that self-regulation, government law, and technologically based control assurance may allay customer concerns. Firms' privacy management requires giving customers at least some control or letting them participate in the future sharing of their personal information (Tucker, 2014). Comparably lax controls over the exposure of personal information can nevertheless lessen people's concerns about their privacy and enhance their propensity to disclose sensitive personal information, even in situations when the actual risks associated with sharing information remain same (Brandimarte et al., 2014). While understanding of privacy controls, it is widely known that, in terms of both the disclosure of personal information and the privacy settings that go along with it, privacy intentions are comparatively poor predictors of actual information disclosure (Acquisti and Grossklags 2005).

Users (consumers) generally become more privacy-conscious with time, and there are notable differences between users reported and desired privacy settings and their actual privacy settings (Lee et al., 2017). Privacy tensions can be exacerbated or reduced by structures like regulatory frameworks, or laws, which can both facilitate and constrain consumer and corporate actions in the digital realm (Quach et al., 2022). Fairness, trust, and responsibility are the goals of privacy regulatory frameworks and policies in the sharing of consumer data with businesses. Major privacy frameworks, like other consumer-focused public policies, aim to balance competing society goals like business profitability and economic development with the protection of people's rights and enhancement of general societal well-being (Davis et al., 2021; Kopalle & Lehmann, 2021). Digital technology has advanced dramatically, simplifying procedures that enable businesses to exchange and profit from customer data but also increasing the complexity of consumer privacy protection. According to Quach et al. (2022), the two primary ways that data protection regulations are typically enforced are through management practices and privacy policies of businesses, which can be classified as more proactive or more reactive. Proactive conditions necessitate more extensive adjustments than reactive situations, which suggest less modifications and less impact on current business structures and performance, while a reactive strategy require notification of data breaches in terms of managerial procedures. It's still a question how consumers' perceive proactive privacy control influencing their intention to disclose personal information. Thus, we hypothesize that

H₂: Online platforms that are perceived to implement effective privacy control (PC) positively influence consumers' intention to disclose personal information (IDPI).

Privacy Information Transparency

There are several levels of information transparency, depending on the kind of privacy information that consumers require. Popular information features satisfy customer needs for privacy information. Among these are a privacy statement or policy that describes how an organization feels about transparency and user-submitted data (Kim et al., 2019). Additional information aspects that cater to different consumer information needs include privacy seals, membership and association with privacy organizations (Feng & Xie, 2014), self-policing procedures and strategies (Xu et al., 2011), data collection information (Bertot et al., 2010), data processing and management (Bonatti et al., 2017; Li et al., 2020), and privacy closures.

According to Agozie and Kaya (2021), attention is focused on the main weaknesses in information openness that have been identified in the literature. Zhou et al. (2018) claim that previous studies on the effect of information transparency in e-media did not examine the specific ramifications of the privacy information antecedents from an information transparency standpoint. Very few people have focused on only one or two variables. For instance, Wang et al. (2016) and Pavlou et al. (2007) investigated security-related topics. The study by Agozie and Kaya (2021) broadens the scope of earlier research by defining privacy information transparency in terms of three dimensions: data collection, data processing, and data use transparency. Furthermore, Granados et al.'s (2008) research provides a way to incorporate relevant studies into a conceptual framework for information transparency. However, they didn't consider privacy concerns related to information or really look into how information openness can influence the behavior of potential users. Zhou et al. (2018) strongly recommend further research on the impact of information transparency on customers.

Numerous research has examined the crucial idea of information transparency in privacy assurance (Ibrahim & Narcyz, 2015; Xu et al., 2011). Openness across a range of contexts, such recommender systems and search engines, for example, shows a structure that makes these systems easier for users to understand. Therefore, consumers may comprehend how a specific input leads to a specific consequence when a system is transparent. Users see these systems as transparent because they get explanations and justifications for the search recommendations and results (Choi et al., 2018; Ibrahim & Narcyz, 2015). On the other hand, information transparency helps to unlock the functionality, service offerings, and process information elements of a platform by making it visible and accessible (Zhou et al., 2018; Xu et al., 2014). In view of the primary facets of user

information management, this might thus satisfy users' information needs (Xu et al., 2014). Research on transparency typically concur that easily accessible, easily comprehensible information satisfies consumers' information needs (Xu et al., 2011). According to Gupta et al. (2020), the idea of information transparency has a strong foundation and is applicable to e-platforms. Customers will start to care about how much personal information is released if they believe they have the right degree of control over information flows, according to Zhou et al. (2018). Customers may therefore restrict contact or decrease disclosure if they believe that service providers are not being entirely genuine about the information they have supplied (Choi et al., 2018). This claim establishes the importance of information transparency in general. However, because electronic platforms are organized and need frequent transparency, users may find it difficult to reduce or stop using them. Consumers may gradually develop emotional fatigue or skepticism towards e-service websites, thereby leading to unwanted privacy practices. Accordingly, the goal of information transparency methods is to ensure that users understand how their participation in, or disclosure of, personal data leads to a particular information output (Bertot et al., 2010). This implies, according to Bansal et al. (2015), that the service provider takes ownership of the duty to reduce operational uncertainty while maintaining the security of client data.

Information transparency, according to Mutimukwe et al. (2019), relates to how easy it is for customers to receive clear and concise information; they must evaluate the reliability of the transactional process and the adherence to security requirements. This description serves as the foundation for the research of the phenomenon of privacy information transparency in e-platforms. Thus, the extent to which users of private information can assess the reliability and privacy assurance protocols of electronic websites. The notion of physical distance between users and e-service systems generally supports the need for information transparency (Obi, 2015; Zhou et al., 2018). The goal of this study is to better understand how customers' intentions to disclose private information are influenced by perceived privacy information transparency (PIT), which acts as a mediator between the two independent variables (privacy turbulence and control). Therefore, we suggest:

H₃: Perceived privacy information transparency (PIT) mediates the relationship between privacy turbulences (PT) and the intention to disclose personal information (IDPI).

H₄: Perceived privacy information transparency (PIT) mediates the relationship between privacy control (PC) and the intention to disclose personal information (IDPI).

Privacy Cynicism

Following conceptualization of cynicism as misalignment of idea or experience that breeds mistrust in a variety of context (Boush et al., 1993; Regoli, 1976), cynicism has been a point discussion among scholars. For instance, cynicism is a result of 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). Other theoreticians point out that cynicism as obstacles and unmet expectations that lead to mistrust (Thompson et al., 1999); it is mistrust that results from unmet requirements and unachievable standards (Choi et al., 2018); it is a link between mistrust and privacy skepticism (Lutz, Hoffmann, & Ranzini, (2020). ; Hoffmann, (2016).) (Lutz et al., 2020). Apart from different explanation of cynicism, scholars agree cynicism is the way that people's growing skepticism affects their views toward adopting and using mobile banking (Chaouali et al., 2017) or any other e-service platforms.

Choi et al. (2018) and Hoffmann et al. (2016) claim that cynicism has also been conceptualized as an additional, novel explanation for the "privacy paradox." Privacy cynicism was characterized by Hoffmann et al. (2016:5) as "an attitude of uncertainty, powerlessness, and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile". A well-established term, privacy cynicism encompasses consumer attitudes regarding privacy, control over personal data, and data protection (Hoffmann et al., 2016). Private data protection, thus, is a component of cynicism and can be related to privacy issues and new technologies. It is currently unclear how privacy cynicism relates to technology use, systems, and how it influences adopting new behaviors, according to researchers (Acikgoz & Vega, 2022). Mechanisms similar to privacy cynicism have been described in the literature before, despite being a relatively new idea. According to Dencik and Cable (2017:15), for instance, surveillance realism is "a simultaneous unease among citizens with data collection alongside the active normalization of surveillance that limits the possibilities of enacting modes of citizenship and of the imagination of alternatives." So, privacy cynicism could help to explain some of the differences between privacy perspectives and fears, as well as privacy actions (Kokolakis, 2017; Lutz et al., 2020). Privacy-cynical persons may adopt such attitudes instead of protecting their privacy as a way to deal with the particular challenges presented by (institutional) privacy concerns (Lutz et al., 2020). Not only do people give the corporate access to their data, but they also assume privacy risks because they don't trust it with their data. In their qualitative panel survey, Hoffmann et al. (2016) identified participants who were privacy skeptical, arguing that privacy protection is meaningless and that this caused them to engage in open or even careless self-disclosure activities. According to Vega & Acikgoz (2022), customers who demonstrate the function of privacy skepticism as a coping technique appear skeptic about privacy and rationalize that they took little effort to secure.

Choi et al. (2018:43) identified privacy cynicism as “an attitude toward (privacy) that is characterized by frustration, hopelessness, and disillusionment” and measured it in their survey-based study. When skepticism (i.e., privacy fatigue) is substantial, the negative relationship between privacy concerns and disclosure intention becomes less evident. Given that privacy cynicism may discourage people from acting even when they have privacy concerns, these findings suggest that privacy cynicism serves as a so-called buffering or contributing moderator (Andersson et al., 2020; Holbert & Park, 2020). In addition, Segijn and Van Ooijen (2020) used the Choi et al. (2018) scale to measure people's skepticism about privacy in a survey-based study conducted in the United States. They found that people's pessimism about privacy was correlated with their acceptance of privacy-invading activities on the internet, like location-based communication, online profiling, and watermarking. As part of the ongoing debate, this study intends at contributing to examine the interaction role of privacy cynicism effect in encouraging or discouraging privacy information transparency in adopting e-services. Hence, we hypothesize that:

H₅: The impact of privacy turbulence (PT) on perceived privacy information transparency (PIT) will strengthen when there is high privacy cynicism (PCc) about using e-services.

H₆: When there is a high level of privacy cynicism (PCc) towards e-services, the impact of privacy control (PC) on perceived privacy information transparency (PIT) will intensify.

H₇: The relationship between perceived privacy information transparency (PIT) and consumers' intention to disclose personal information (IDPI) will decline when there is a high influence of perceived privacy cynicism on online platforms.

II. Method

Design

According to Welman and Kruger (2005), research design is a thorough strategic plan that outlines a researcher's approach to recruiting research participants and collecting data from them, with an eye toward sampling techniques and the corresponding survey approach. For the sake of generalizability, the study intends to use probability sampling to gather data from a sizable sample that accurately represents the group being studied. Couper (2000: 465–466) may have expressed it best when it came to web-based surveys when he stated that “web-survey approach must be done in the context of its intended purpose and the claims it makes.” Cross-sectional data allows for the cost-effective collecting of data from a population and can be generalized based on individual or group observations (Research methods for business students., 5th ed., Pearson Education Limited)(Saunders et al., 2009). Each system can employ exploratory, descriptive, or explanatory research, depending on the study's objectives (Yin, 2003). As a result, the objectives of the study call for an explanatory survey to ascertain the causal influence of the mediated and moderated interactions (Saunders et al., 2009).

About 25% of the 36.8 million users of the Tele Birr app, according to experts, are based in Addis Ababa, the country's capital. The study's population, according to the company's usage of media reports, is estimated to be 1.4 million online service customers, with 1.08 trillion in transactional values in 2023. In order to enable appropriate sampling, Saunders et al. (2009) state that the sampling frame should give a thorough, up-to-date, and accurate representation of every case the study intends to examine. While aiming for the whole population would be intriguing, time and financial limits make it impractical. According to the literature, researchers can ensure validity by creating a sampling frame specifically for the study when one is not available (Saunders et al., 2012); they can also conduct marketing research from a population at a lower cost even in cases where the sampling frame is indefinite (Kotler & Armstrong, 2015).

Sampling and Data Collection Procedures

The goal of the study is to use probability sampling by non-list-based random sampling, as opposed to the conventional method of telephone surveys that involves counting the sample frame through random digital dialing (RDD). The intercept survey (Saunders, 2014; Dillman et al., 2014; Walgrave and Verhulst, 2011) often involves systematic sampling of visits from online retailers, online service providers, and shopping malls because the RDD couldn't fit into a web-based survey. Systematic random sampling, in which the next client is chosen using the intercept survey technique at regular intervals after the first sampling point is chosen at random (Couper, 2000).

The researchers chooses to create 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. The capital geographic location is divided into ten sub-cities (Bole, Yeka, Akaki-kaliti, Nfas Silk, Kofe-Keranio, Gullel, Addis Ketema, Arada, Lideta, and Krkos). To work in the four study panels (NE, NW, SE, and SW), twelve research assistants were selected from among Addis Abeba University students, with each panel having an equal workload of 115–116 respondents to recruit. To specific e-service providers, each research panel allocates three research assistants. 335 consumers' data (73% response rate) with a female-to-male ratio of 49:51 was obtained, compared to the anticipated sample size of 462. Dillman (2007) and Ballantyne (2005)

found that online surveys had response rates ranging from 35% to 47%, which was higher than the 50% recommended by Mendenhall and colleagues (2003). According to the literature review, which includes works by authors like Dillman et al. (2014), Saunders (2014), Walgrave and Verhulst (2011), and others who support the intercept sampling approach as a workable and beneficial method given the chance to gain consent and customers' willingness to participate in the survey, the researcher's data collectors were trained to select the first customer, and then the next intercept customer to be the fifth, 10th, 15th, and so forth for 8 working hours for consecutive five days at their respective assigned e-service provider. For unwilling clients, the researchers suggest a pattern of five plus one; if the customer declines once again, the researchers advise the research assistants to go to the next eligible (regular fifth) customer during the training session.

Instruments

A critical evaluation of the literature was done in comparison to the study's variables. In order to create the questionnaire, make measurements, and assume strong correlations between the variables, a rigorous examination of the literature on the variables was conducted, adhering to the recommendations of Ghauri and Grnhaug (2010). The survey items were somewhat altered in accordance with the particular research need, and the variables were taken from earlier studies. Customers are rated according to their opinions and/or experiences with using online platforms using a five-point Likert scale that ranges from "strongly disagree" to "strongly agree." Petronio (2002, 2013): three items measurement on privacy turbulence; Malhotra et al. (2004): three items measurement on privacy control; Choi et al. (2018): three items on privacy cynicism; Agozie & Kaya, 2021: four item tools for measuring privacy information transparency; and Malhotra et al. (2004): three items measuring the intention to disclose personal information have been adopted.

III. Findings

Descriptive Statistics

Descriptive data and bivariate correlations for independents, mediators, moderators, controls, and outcome variables are presented in Table 1. With an age standard deviation of 9.67, the data is more dispersed relative to the mean, particularly in the 18–71 age group. The controlling variables show how the study's variables are controlled. The outcome variable—consumers' desire to disclose personal information, implying the direction and extent of relationships—correlates significantly with perceived privacy turbulence (e.g., $r = .182, p = .01$) and personal information transparency (e.g., $r = .133, p = .05$). The independent variables of privacy control and privacy information transparency have significant correlations ($r = .113, p = .05$), indicating a statistical relationship between them. Privacy control was found to have an insignificant correlation with the outcome variable (e.g., $r = .052, p < .05$), allowing opportunity for more investigation because correlation does not imply causation.

Table 1: Pearson’s Correlation

Correlations											
	Mean	Stand. Dev.	N	Sex	Marit. Status	Age	Av_PT	Av_PC	Av_PCC	Av_PIT	Av_IDPI
Sex	1.5	.50	335	1							
Marital	1.8	.85	335	-.101	1						
Age	37.4	9.67	335	-.012	.464**	1					
Av_PT	4.4	.72	335	.152**	.062	.095	1				
Av_PC	4.3	.81	335	.079	.046	.102	.440**	1			
Av_PCC	2.5	1.48	335	-.016	-.011	.026	.077	-.023	1		
Av_PIT	3.5	1.10	335	-.012	.178**	.171**	-.097	.113*	.108*	1	
Av_IDPI	3.4	1.24	335	.027	.187**	.125*	.182**	.052	.130*	.133*	1
**. Correlation is significant at the 0.01 level (2-tailed).											
*. Correlation is significant at the 0.05 level (2-tailed).											

Reliability and Validity Tests

According to Brown (2015), the item variance in factor loading is displayed using the Explanatory Factor Analysis (EFA) that employs the communality extraction factor. According to Beavers et al. (2013), 0.7 and above is the optimal communality range, and a cutoff measure of .25 to .4 was proposed. Twelve constructs represent the optimal range for communalities, according to Annex 1, with the remaining four (PC3 = .571, PT2 = .643, PT3 = .609, and PIT1 = .612) recording slightly below the ideal cutoff but over the recommended acceptable range. The

reliability tests confirmed the coefficient ranging from .703 - .923; in accordance with Hair et al. (2010), the constructs are deemed reliable if their Cronbach's alpha (α) value is 0.7 or higher in reliability testing.

Additional analysis was suggested by Fornell and Larcker (1981). Construct reliability (CR) surpasses the 0.7 threshold; 2) the standardized regression weight exceeds 0.7 at the $p < .05$ or $p < .01$ significance level; and 3) the average variance extracted (AVE) predicts the variance between latent indicators more than 0.5. Thirteen of the sixteen items in Annex 1 have standardized factor loadings that are higher than the cut-off value of 0.7, and three items are nearer this threshold. Additionally, as shown in Annex 1, the average variance extracted (AVE) is greater than the suggested value, and the construct reliability (CR) values vary from .751 to .924 within the suggested threshold. As a result, our study suggests that convergent validity is eligible, which opens the door for discriminant validity.

The EFA and the CFA need to be looked at in order to analyze discriminant validity. First, the Kaiser-Meyer-Olkin (KMO) sample adequacy test evaluates the sample's capacity to assign items to factors (Kaiser, 1974). Standard indicators to confirm or decline sample adequacy are KMO values, which range from above the 0.8 to 0.6 cutoff (Beavers et al., 2013). With a degree of freedom of 120, a p-value of .000, a Chi-Square approximation of 3473.3, and an outcome that falls within the desired range (.687), the sample size is deemed suitable. The cumulative variance of the interpretation rate after seven items are rotated is 76.69%, which is more than 50% of the recommended value and indicates that the research data is effectively extracted. The estimations of the factor loading coefficient of all the constructs' items surpass 0.7. To further support discriminant validity, each square root of AVE is larger than the correlation coefficient (Table 2) (Fornell and Larcker, 1981). The approval of measurement items for discriminant validity is contingent upon the presence of both types of evidence.

Table 2: Pearson's Correlation and Square Root of AVE

	Av_PT	Av_PC	Av_PCc	Av_PIT	Av_IDPI
Av_PT	.713				
Av_PC	.440**	.725			
Av_PCc	.077	-.023	.896		
Av_PIT	-.097	.113*	.108*	.771	
Av_IDPI	.182**	.052	.130*	.133*	.909
** . Correlation is significant at the 0.01 level (2-tailed).					
* . Correlation is significant at the 0.05 level (2-tailed).					

Note: Diagonal bolded values show the square root of AVE

Analysis of Common Methods Variance

Common method variance (CMV) can be problematic for behavioral research (Podsakoff et al., 2003). It verifies whether noise is present on the instrument or not (Chang and Eden, 2010). To identify a common element, we looked at the study's variables: customers' privacy turbulence, control, transparency of personal information, cynicism, and intention to disclose personal information. The greatest variance in this investigation was 21.99% on any one factor, in accordance with the advice of Podsakoff and colleagues to do an EFA test of common method bias using Harman's single component analysis. The results indicate that there are no CMV-problems with the dataset for testing hypotheses because the suggested overall variation for a single element shouldn't be greater than 50%. To ensure a strong validation of CMV, an extra examination was conducted utilizing the Pearson's correlation method, as recommended by Bagozzi et al. (1991). Table 2 clearly shows that there was no pathological threat of CMV, with correlations between any of the study's variables being substantially less than 0.9.

Hypotheses Testing

Direct Hypotheses

An output summary of Model 58's causal conclusions about the percentile of 10,000 bootstrap samples with a 95% confidence interval is provided by Hayes' (2018) PROCESS procedure model for SPSS version 3.5.3. The first two hypotheses examine the factors that precede customers' intention to disclose personal information. The empirical evaluation of perceived privacy turbulence and control are two variables that could have antecedent relations to consumers' intention to disclose personal information. The SPSS run computations presented in Annex 2 confirm hypothesis H1 (privacy turbulence) and are unable to support H2 (privacy control). Accordingly, there is a significant causal relationship (H1) between privacy turbulence and consumers' intention to disclose personal information [$\beta = .414$, $p = .000$, CI [.241 to .581] using model specification $R^2 = .174$, $F(4, 330) = 17.39$, p -value = .000; however, the causal relationship between privacy control and the intention to disclose personal

information represented by H2 was found to be statistically insignificant [$\beta = .125, p > .05, CI [-.032 \text{ to } .282]$ and model specification $R^2 = .125, F(4, 330) = 11.80, p\text{-value} = .000$], inferring the relationship could not be supported.

Mediating Hypotheses

The study adopted the bootstrapping procedures for the mediation test, based on Zhao et al. (2010). As a result, we used 10,000 bootstrap samples at a 95% confidence interval (CI) as an indication to assess the mediation of the privacy information transparency model.

Table 3 presents the results indicating privacy turbulence (PT) has a significant effect on both privacy information transparency (PIT) and consumers' intention to disclose personal information (IDPI) (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 ($\beta = -.121$ at 95% CI $[-.343 \text{ to } -.103]$) exerts a significant indirect effect on privacy vulnerability and consumers' intention to disclose personal information. Thus, the predicted relationship (H3) is tenable on the mediator role of privacy information transparency between the privacy turbulence and consumers' intention to disclose personal information. Overall, the result provides empirical support for the PIT's mediation between privacy turbulence (PT) and the intention to disclose personal information (IDPI).

Table 3: Mediation Test of Hypothesis – H3

Hypothesis: H3	(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		6.242	.824	.000		-1.16	.583	.048	
Av_PT	a	-.634	.176	.000	c	.414	.088	.000	
PIT					b	.715	.102	.000	
Bootstrap Indirect Effect		Effect	Boot SE	LL 95% CI		UL 95% CI			
PT → PIT → IDPI		-.121	.061	-.343		-.103			
		R ² = .049 F(3, 331) = 5.709, p-value = .001				R ² = .174 F(4, 330) = 17.39, p-value = .000			

The research predicts privacy information transparency has a mediating role between privacy control (PC) and consumers' intention to disclose personal information (IDPI), indicated by H4, in accordance with Judd and Kenny (1981) and Kenny et al. (1998), the causal sequential phase of the mediation process. A bootstrap of 10,000 samples with a 95% confidence interval (CI) was used to conduct the test. According to Table 4, privacy control had a negligible impact on the mediator (PIT) and a negligible impact on the dependent variable—the intention to expose personal information. To summarize, the indirect impact paths of mediation bootstrap revealed a statistically negligible effect ($\beta = .017$ at CI $[-.004 \text{ to } .050]$), which was not able to provide empirical support for the hypothesized link (H4 - PIT mediates the interactions between PC and IDPI).

Table 4: Mediation Test (H4)

Hypothesis: H4	(Mediator) Privacy Information Transparency (PIT)		(DV) Privacy Protective Behavior (PPB)			Decision			
Antecedents (IVs)	Path	Coeff.	SE	p-value	Path	Coeff.	SE	p-value	Not Supported
Constant		3.79	.782	.000		.392	.525	.456	
Av_PC	a	-.095	.171	.581	c	.125	.080	.117	
PIT					b	.631	.103	.000	
Bootstrap Indirect Effect		Effect	Boot SE	LL 95% CI		UL 95% CI			
PC → PIT → IDPI		.017	.014	-.004		.050			
		R ² = .033 F(3, 331) = 3.724, p-value = .012				R ² = .125 F(4, 330) = 11.805, p-value = .000			

Moderating Hypotheses

The goal of the study is to investigate two moderation hypotheses (H5 and H6) between the independent variables, privacy turbulence and control, and the mediating variable, personal information transparency (PIT). The results of the exploration, using Hayes (2018) PROCESS method Model 58, are appended in Annex 2.

A moderation test was conducted to examine the relationship between the privacy turbulence (PT) and personal information transparency (PIT), with privacy cynicism (PCc) acting as a moderator, represented by H5. In particular, there are negative coefficients, referring Table 5, PT to PIT, and PCc to PIT. Regression weights of the interaction effect of PT*PCc $\beta = .206, t = 3.084, p = .003$, and CI $[.073 \text{ to } .340]$ distinct from zero at a 95% confidence range of 10,000 samples indicated the presence of a significant effect. In addition, the model test

appeared statistically significant indices of $\Delta R^2 = .049$ and $F(3,331) = 5.79, p = .000$. As a result, the tests corroborated and validated the hypothesized relationship. Based on these findings (Table 5), the study came to the conclusion that H5 - privacy cynicism moderates the relationship between the privacy turbulence and transparency of privacy information.

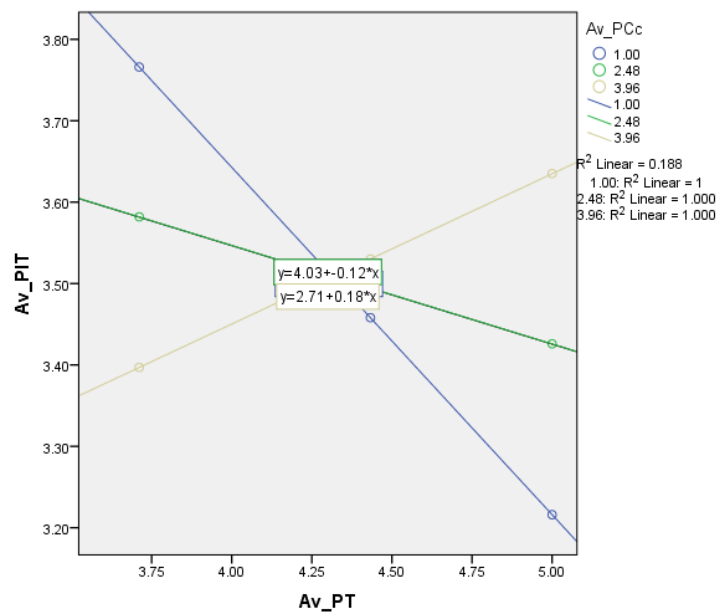
Table 5: Analysis of Interaction Effect Hypotheses H5 & H6

	Variables	β	SE	t	p	LLCI	ULCI	Decision
H5	Intercept	6.242	.824	7.572	.000	4.621	7.864	Supported
	PT \rightarrow PIT	-.677	.176	-3.603	.000	-.979	.288	
	PCc \rightarrow PIT	-.891	.324	-2.748	.006	-1.528	-.253	
	PT*PCc (Int_1)	.206	.068	3.0837	.003	.073	.340	
	R ² Change	.049**						
	F	5.709						
H6	Intercept	3.786	.758	4.844	.000	2.248	5.323	Supported ³
	PC \rightarrow PIT	-.095	.171	-.553	.581	-.432	.242	
	PCc \rightarrow PIT	-.320	.252	-1.272	.204	-.815	.175	
	PC*PCc (Int_2)	.088	.054	1.619	.106	-.019	.194	
	R ² Change	.033*						
	F	3.724						

*p < .05 **p = .000

The syntax of a conditional interaction effect graph showing low (blue), medium (green), and high (brown) levels of privacy cynicism effect in the predictor privacy turbulence (PT) and dependent variable privacy information transparency (PIT) was generated using the Hayes (2018) SPSS-PROCESS macro version 3.5.3 as a robust check and cross-validation. A high sense of perceived privacy cynicism (PCc) in comparison to low and medium perceptions is shown in Graph 1 where PCc has opposite slopes. Based on the data shown in Table 5, it can be determined that there is a statistically significant causal-effect relationship. As a result, the hypothesis designated H5 suggests that there is enough data to validate the proposed association.

Figure 1: Moderation of Privacy Cynicism between privacy information transparency and privacy turbulence – H5



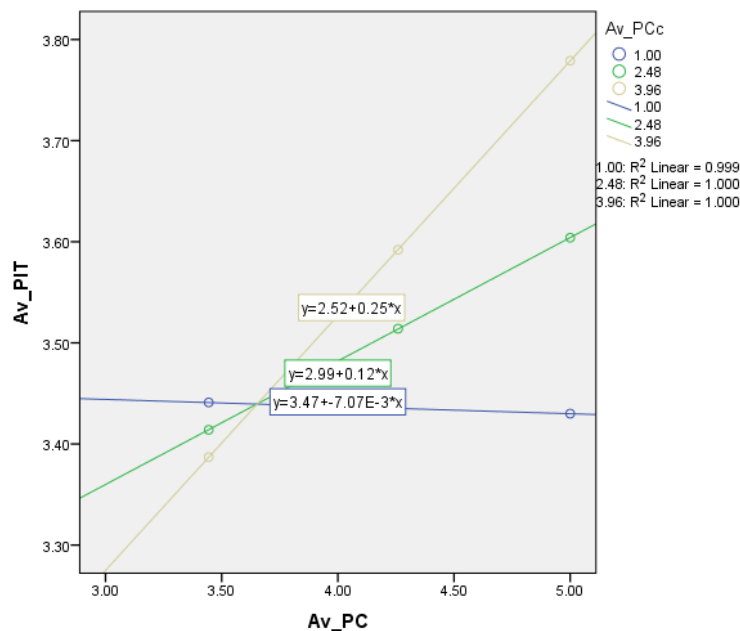
The relationship between privacy turbulence (PC) and personal information transparency (PIT) was investigated through a moderation test, in which privacy cynicism (PCc), represented by H6, acted as a moderator. With statistically insignificant correlations included, privacy control (PC) exhibits a negative regression coefficient (β

³ Supported after graphic probing

= -.095, $t = -.553$, $p > .05$, and CI [-.0432 to .242]. Similarly, there is a statistically negligible correlation between privacy cynicism and privacy information disclosure, with a zero confidence interval [-.815 to .175]. Regression weights of the interaction effect of PC*PCc, $\beta = .088$, $t = 1.619$, $p > .05$, and CI [-.019 to .194] not distinct from zero at a 95% confidence range of 10,000 samples that indicated the presence of an insignificant effect. With indices of $\Delta R^2 = .033$ and $F(3,331) = 3.724$, $p < .05$., the model test seems to be statistically significant. Thus, Table 5's findings indicate that the hypothesized link—H6—that privacy cynicism moderates the relationship between privacy control and transparency of privacy information—is not supported empirically.

Despite this, further investigation is necessary to determine whether or not the interaction effects are substantial and whether or not the interaction coefficient's sign indicates the necessary information. Different probing steps are advised by many researchers. For example, Jaccard (2001) recommends including a straightforward slope or effect coefficient line graph; Hayes and Matthes (2009) provide guidance on how to consider variance across group differences when doing the Johnson-Neyman test; and Aiken and West (1991) propose a mean-centered approach to predictors. In order to determine the list of data to visualize conditional effect syntax in order to plot the moderation impact, we have implemented the PROCESS Hayes (2018) version 3.5. The degree of X (independent) conditional effect as a function of M (moderator) is what is involved in investigating an interaction (Hayes, 2018). Hayes offers guidelines for a conditional estimate effect of X for any value of M, and interaction displays a slope that is statistically distinct from zero in order to actualize the moderating effect. As a result, figure 2 provides a visual depiction of interaction effects and hypothesis testing analyses. Using an SPSS-generated graph, it demonstrated that the expected hypothesis is supported: privacy cynicism (PCc) moderates the link between privacy control (PC) and privacy information transparency (PIT).

Figure 2: Moderating Effect of Privacy Cynicism between Privacy Control and Privacy Information Transparency – H6



A continuation of our discussion on Model 58 of Hayes (2018) PROCESS procedure, the result of the examination is annexed in annex 2. Hypothesis 7 (H7) examines the relationship between privacy information transparency (PIT) and consumers' intention to disclose privacy information (IDPI) with moderation effect of privacy cynicism (PCc). Specifically, the predicted relationship attests that higher influence of privacy cynicism (PCc) declines the relationship between privacy information transparency (PIT) and consumers' intention to disclose personal information (IDPI). There was a significant main effect found between PIT and IDPI, with regression weights of $\beta = .631$, $t = 6.324$, $p = .000$, and CI [.428 to .834] 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 $\beta = -.199$, $t = -5.879$, $p = .000$, and CI [-.266 to -.133]. Besides, the indices of $\Delta R^2 = .125$ and $F(4,330) = 11.805$, $p = .000$, were statistically significant to test the unconditional interaction effect. Thus, the tests confirmed and supported the predicted relationships. From these results (Table 6), the study concluded that privacy information transparency and the intention to disclose personal information are moderated by privacy cynicism to support the hypothesis.

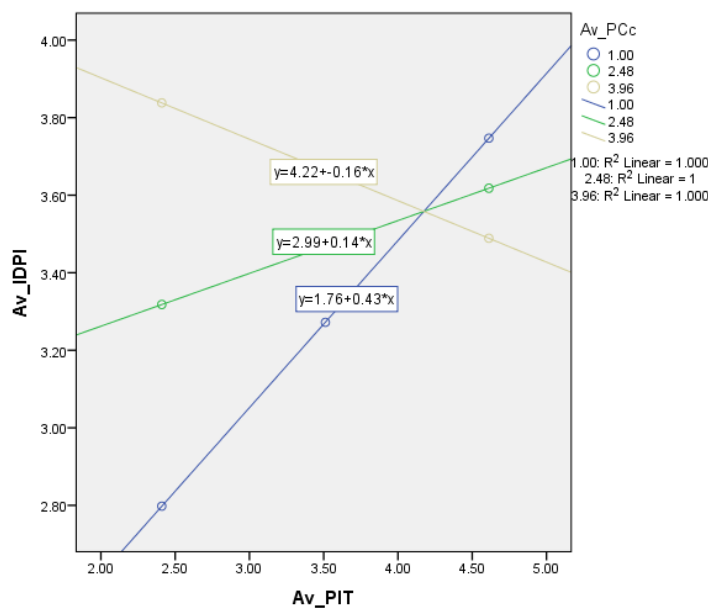
Table 6: Analysis of Interaction Effect Hypothesis H7

Variables	β	SE	t	p	LLCI	ULCI	Decision
H7 Intercept	.392	.525	.746	.456	-.641	1.425	Supported
PIT \rightarrow IDPI	.631	.103	6.107	.000	.428	.834	
PCc \rightarrow IDPI	.831	.131	6.324	.000	.573	1.090	
PIT*PCc (Int_1)	-.199	.034	-5.897	.000	-.266	-.133	
R ² Change	.125**						
F	11.805						

*p < .05 **p = .000

The moderating of the declining relationships between privacy information transparency (PIT) and consumers' intention to disclose personal information (IDPI) is visualized in Figure 3, where privacy cynicism has a bigger influence. The variation depicts relations between PIT and IDPI relationships when PCc is high influence in brown and low influence in blue lines.

Figure 3: Moderating Effect of Privacy Cynicism between Privacy Information Transparency and Consumers' intention to disclose personal information – H7



IV. Discussion and Implications

The study aims to examine discrepancies of privacy turbulence, control, and information transparency on consumers' intention to disclose personal information with the moderation effect of privacy cynicism. The focus was to determine the antecedents of the intention to disclose personal information, the mediation effect of privacy information transparency between the independent and outcome variables, and the moderation effect of privacy cynicism.

The findings are in line with the hypotheses that derived from privacy literature and earlier empirical privacy studies. The extent of the privacy turbulence effect was tested, taking into account its influence on consumers' intentions to disclose personal information. The findings supported the hypothesized function of privacy turbulence on the intention to disclose personal information. The assertion is consistent with privacy turbulence is due to absence, adjustment, and review of privacy regulation becoming a privacy problem (Child and Starcher, 2017; Child et al., 2011; DeGroot and Vik, 2017). However, the extent of privacy control influence on consumers' intention to disclose personal information remained empirically insignificant to the suggested hypothesis. The finding is backed by the previous literature: consumers expect protection, either technological or government regulation, to allay privacy (Xu, 2007); some mechanisms to assure personal information (Tucker, 2004). In sum, perceived privacy turbulence significantly affects consumers' intention to disclose personal information, and without privacy control, people wouldn't feel comfortable sharing their personal information.

Personal information transparency is open to several ramifications of privacy information (Zhou et al., 2018), issues of security (Wang et al., 2016), and is subjectively exposed during data collection, processing, and transparency in data use (Agozie & Kaya, 2021). Consumers' transparency on personal information mostly

intervenes when they perceive privacy turbulence that, in turn, affects their intention to disclose personal information. Thus, this study confirms the mediating role of personal information transparency between privacy turbulence and consumers' intention to disclose personal information. The prevalence of privacy turbulence becomes a source of consumers' hesitation to disclose personal information via personal information transparency, consistent with the literature that says consumers require explanation and justification to disclose personal information, among others, Choi et al. (2018); Ibrahim & Narczyk (2015). On the other hand, the mediation role of personal information transparency between privacy control and the intention to disclose personal information has no empirical support for the predicted relationship. Our findings indicate that consumers' perceived privacy control is unable to stimulate personal information transparency that also affects their intention to disclose personal information. Backing to previous findings, the occurrence of actual or perceived risk affects information disclosure (Brandimarte et al., 2014); absence of privacy control is a predictor against self-disclosure (Acquisti and Grossklags, 2004). Contrary to our expectation, the findings portray that the actual risk of privacy control triggers hesitation toward personal information transparency that leads to a clash with the consumer's intention to disclose personal information.

The results also shed light on moderation tests of privacy cynicism at multiple scenarios as outlined on model 58 of Hayes (2018). Each privacy cynicism moderation tests, a) between privacy turbulence and personal information transparency, b) between privacy control and personal information transparency, c) between personal information transparency and consumers' intention to disclose personal information, were statistically significant on privacy-attitude and management online platforms. This demonstrates several insights for online platforms with the critical interaction effects of privacy cynicism literature. As noted, privacy cynicism emanates due to unfulfilled expectation or disappointment (Choi et al., 2018, Lutz et al., 2020); mistrust (Thompson et al., 1999); unachievable standards (Choi et al., 2018); skepticism (Lutz et al., 2020) that the study build upon existing knowledge on privacy cynicism focusing on its interaction effect on personal information transparency and privacy turbulence, control, and intention to disclose personal information.

Theoretical Implications

Prior researchers have extensively discovered privacy turbulence (Petronio & Child, 2020; DeGroot & Vik, 2017; Child & Starcher, 2017; Child et al., 2011; Petronio, 2002; Petronio & Durham, 2008; Petronio & Bantz, 1991), privacy control (Lee et al., 2017; Stone et al., 1983; Kim et al., 2019; Tucker, 2014; Brandimarte et al., 2013; Xu, 2007; Brandimarte et al., 2014; Lee et al., 2017; Quach et al., 2022; Davis et al., 2021; Kopalle & Lehmann, 2021), privacy cynicism (Boush et al., 1993; Regoli, 1976; Andersson, 1996; Choi et al., 2018; Lutz et al., 2020; Thompson et al., 1999; Chaouali et al., 2017; Hoffmann et al., 2016; Acikgoz & Vega, 2022; Dencik & Cable, 2017; Kokolakis, 2017; Vega & Acikgoz, 2022; Andersson et al., 2020; Holbert & Park, 2020; Segijn & Van Ooijen, 2020), personal information transparency (Kim et al., 2019; Bonatti et al., 2017; Li et al., 2020; Agozie & Kaya, 2021; Zhou et al., 2018; Wang et al., 2016; Ibrahim & Narczyk, 2015; Xu et al., 2011; Xu et al., 2014; Gupta et al., 2020; Choi et al., 2018; Mutimukwe et al., 2019; Obi, 2015), and intention to disclose personal information (Cozby, 1973; Zeng et al., 2020; Moon, 2000; Goldfarb & Tucker, 2011; Martin et al., 2017; Utz, 2015; Fennis et al., 2009; Khan et al., 2011; Hui et al., 2007; Bao & Ni, 2017). Yet, insufficient attention has been given to such a research model, model 58, which poses a major impediment to online platform privacy challenges. To our knowledge, our study attempts to fill previous research gaps identified on online services, focusing discrepancies on perceived privacy turbulence, control, and personal information transparency effect on consumers' intention to disclose personal information with moderation effect of privacy cynicism that building on existing research. In particular, the moderation effect of privacy cynicism at different levels of the study's variables—between independent variables and mediating variables—and also between mediating construct and outcome construct, and therefore contributes to an ongoing body of knowledge on privacy attitude, processes, mechanisms, and management.

Practical Implications

Our study results set important managerial implications for online platforms. The findings suggest that privacy turbulence is recognized as a useful feature and therefore there should be a continued effort to mitigate any perceptions of turbulence as it has a direct influence on consumers' intentions to disclose personal information. On the other hand, online platforms should offer minimum focus on privacy control because its effect on consumers' intention to disclose personal information was found insignificant. For instance, consumers often seek high levels of privacy control on online platforms that alleviate their intention to disclose personal information. Hence, online platform providers are expected to introduce technological shields or regulations to safeguard consumers' information.

Consumers' personal information transparency enhances with confidence when they perceive the online platform's actions are in place. Excessive privacy turbulence via personal information transparency affects consumers' intentions to disclose personal information. Such customer needs are an input to improve the

effectiveness of online platforms and value the experience with them. The privacy cynicism moderation role has a significant interaction effect with the study's variables. Practitioners can take into consideration issues that directly or indirectly become sources of online platform cynicism. The higher influence of privacy cynicism declines the relations between privacy turbulence and information transparency, which could be affecting the goodwill of online platforms. Managers can devise tools on how to reduce privacy cynicism of their respective online platform, such as improvement on privacy management and transparency in privacy information usage.

Limitations of the Study

Despite these implications, coming research on these subjects is needed to overcome several limitations of this study. The limitations of the present study are most directly related to the participant sample from a single country. While we believe that it is representative for online customers, the homogeneity of our sample makes it difficult to extend our findings to the general population from different cultures. Given this fact of diversifying samples, upcoming research should encompass a cross-cultural context to extend our scope of understanding. In addition, this study mainly focused on the quantitative method; thus, we suggest other research methodologies such as case study, qualitative, experimental study, longitudinal, and mixed approach to widen our know-how. Additionally, we use limited privacy constructs that can be enriched by adopting other variables such as privacy security (De Wolf, 2020), privacy vulnerability (Dunbar et al., 2021), and privacy concern (Acikgoz and Vega, 2022; Zhang et al., 2022). By taking all these factors into account, future research can add value by coming up with research models portraying the causal complexity of privacy issues.

V. Conclusions

The study addressed three objectives. First, it assessed the direct link of privacy turbulence (privacy control) to consumers' intention to disclose personal information. We find that privacy turbulence has a statistically significant effect on the intention to disclose personal information, while the privacy control was unable to support empirically. The second component focused on the mediation effect of personal information transparency that has revealed mixed outcomes. It significantly mediated between the privacy turbulence and the intention to disclose personal information. On the other side, personal information transparency was found to have an to have an insignificant mediation effect between privacy control and the intention to disclose personal information. The third part focused on the moderation effect of privacy cynicism at different levels of the conceptual framework, Hayes' (2018) model 58, that three tests carried out revealed statistically significant relationships.

References

- [1]. Abdelmoety, Z. H.-D. (2022). A cross cultural investigation of retailers commitment to CSR and customer citizenship behaviour: The role of ethical standard and value relevance.
- [2]. Acikgoz, F. &. (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. .
- [3]. Acquisti, A. B. ((2020).). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, 30(4), 736–758. Portico. Retrieved from <https://doi.org/10.1002/jcpy.1191>
- [4]. Acquisti, A., & Grossklags, J. ((2005).). Privacy and rationality in individual decision making. . *IEEE Secur. Priv.* 3, 26–33.
- [5]. Agozie, D. Q. (2022). Do communication content functions drive engagement among interest group audiences? An analysis of organizational communication on Twitter. *Humanities and Social Sciences Communications*, 9(1). Retrieved from <https://doi.org/10.1057/s41599-022-01275-5>
- [6]. Agozie, D. Q. (2022). Environmental Kuznets Curve hypothesis from lens of economic complexity index for BRICS: Evidence from second generation panel analysis. *Sustainable Energy Technologies and Assessments*, 53, 102597. Retrieved from <https://doi.org/10.1016/j.seta.2022.102597>
- [7]. Agozie, D., & Kaya, T. ((2021)). Discerning the effect of privacy information transparency on privacy fatigue in e-government. . *Gov. Inf. Q.* 38, 101601.
- [8]. Alzaidi, M. S. ((2022)). The Role of Trust and Privacy Concerns in Using Social Media for E-Retail Services: The Moderating Role of COVID-19. *SSRN Electronic Journal*. Retrieved from . <https://doi.org/10.2139/ssrn.4068666>
- [9]. Anderson, C. a. ((2011).). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, Vol. 22 No. 3, pp. 469-490.
- [10]. Andersson, U. C.-C. ((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).
- [11]. Bagozzi, R. Y. ((1991).). Assessing Construct Validity in Organizational Research. *Administrative Science Quarterly*, 36(3), 421–458.
- [12]. 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 Reachin.
- [13]. 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 Reachin.
- [14]. Bansal, G. Z. ((2015)). Do context and personality matter? Trust and between expressed privacy concerns and actual online behavior . A systematic literature review. *Telematics and Informatics*, 34, 1038–1058.
- [15]. Bao, W. &. ((2017)). Could Good Intentions Backfire? An Empirical Analysis of the Bank Deposit Insurance. *Marketing Science*, 36(2), 301–319. Retrieved from <https://doi.org/10.1287/mksc.2016.1009>
- [16]. Beavers, A. S. ((2013).). Practical considerations for using exploratory factor analysis in educational research, *Pract. Assess. Res. Eval.* 18, 1 (2013).

- [17]. Bellman, S. J. ((2004)). International Differences in Information Privacy Concerns: A Global Survey of Consumers. . The Information Society, 20(5), 313–324. Retrieved from <https://doi.org/10.1080/01972240490507956>
- [18]. Bertot, J. C. ((2010).). Social media technology and government transparency. . Computer, 43(11), 53–59.
- [19]. Bonatti, P. K. ((2017).). Transparent personal data processing: The road ahead. In S. Tonetta, E. Schoitsch, & F. Bitsch (Eds.), 10489. . Computer safety, reliability, and security. SAFECOMP 2017. Cham: Springer.
- [20]. Boush, D. M. ((1993)). Cynicism and conformity as correlates of trust in product information sources. . Journal of Current Issues & Research in Advertising, 15(2), 71–79.
- [21]. Brandimarte, L. A. ((2013)). Misplaced Confidences. Social Psychological and Personality Science, 4(3), 340–347. Retrieved from <https://doi.org/10.1177/1948550612455931>
- [22]. Brown, T. A. ((2006).). Confirmatory factor analysis for applied research. . New York: The Guilford Press.
- [23]. Chang, S. a. ((2010).). From the editors: common method variance in international business research. . Journal of International Business Studies, Vol. 41 No. 2, pp. 178-184.
- [24]. Chaouali, W. S. ((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. .
- [25]. Child, J. &. ((2010).). Unpacking the Paradoxes of Privacy in CMC Relationships: The Challenges of Blogging and Relational Communication on the Internet.
- [26]. Child, J. &. ((2013)). Let's Be Facebook Friends: Exploring Parental Facebook Friend Requests from a Communication Privacy Management (CPM) Perspective. . Journal of Family Communication, 13, 46 - 59.
- [27]. Child, J. &. ((2016)). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. Comput. Hum. Behav., 54, 483-490.
- [28]. Child, J. H. ((2012).). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. Comput. Hum. Behav.
- [29]. Child, J. P. ((2009)). Blogging, communication, and privacy management: Development of the Blogging Privacy Management Measure. J. Assoc. Inf. Sci. Technol., 60, 2079-2094.
- [30]. Choi, H., Park, J., & Jung, Y. ((2018).). The role of privacy fatigue in online privacy behavior. . Comput. Hum. Behav. 81, 42–51.
- [31]. Choi, S. M. (2020). To Err Is Human(-oid): How Do Consumers React to Robot Service Failure and Recovery? . Journal of Service Research.
- [32]. Couper, M. ((2000).). Web surveys: A review of issues and approaches. . Public Opinion Quarterly, 64, 464-494.
- [33]. Cozby, P. C. ((1973)). Self-disclosure: A literature review. Psychological Bulletin, 79(2), 73–91. Retrieved from <https://doi.org/10.1037/h0033950>
- [34]. Davis, B. G. ((2021)). The future of marketing analytics and public policy. . Journal of Public Policy & Marketing, 40(4), 447–452.
- [35]. De Wolf, R. ((2020)). Contextualizing how teens manage personal and interpersonal privacy on social media. . New Media Soc. 2020, 22, 1058–1075.
- [36]. DeGroot, J. a. ((2017)). We were not prepared to tell people yet: confidentiality breaches and boundary turbulence on Facebook. Computers in Human Behavior 70: 351–359.
- [37]. Dencik, L. &. ((2017).). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. . Journal of International Communication, 11, 763–781.
- [38]. Dillman, D. ((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.
- [39]. Dillman, D. A. ((2014).). Internet, phone, mail, and mixed-mode surveys: . The tailored design method (4th ed.). Hoboken, NJ: Wiley.
- [40]. Dunbar, J., 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.
- [41]. Feng, Y. &. ((2014)). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy protecting behavior. Computers in Human Behavior, 33, 153–162.
- [42]. Fennis, B. M. (2009). Acts of Benevolence: A Limited-Resource Account of Compliance with Charitable Requests. A Limited-Resource Account of Compliance with Charitable Requests. Journal of Consumer Research, 35(6), 906–924. Retrieved from <https://doi.org/10.1086/593291>
- [43]. Fornell, C. &. ((1981)). Evaluating structural equation models with un- observable variables and measurement error. . Journal of Marketing Research, 18(1) 39-50.
- [44]. Fornell, C. &. ((1981).). Evaluating structural equation models with un- observable variables and measurement error. Journal of Marketing Research, 18(1) 39-50.
- [45]. Gauri, P. &. ((2010).). Research Methods in Business Studies: A Practical Guide. (Fourth Edition ed.) FT-Pearson.
- [46]. Ginder, W. &-E. ((2022)). To trust or not to trust? The interplay between labor-related CSR claim type and prior CSR reputation of apparel retailers. Journal of Retailing and Consumer Services, 65, 102875. . Journal of Retailing and Consumer Services, Retrieved from <https://doi.org/10.1016/j.jretconser.2021>
- [47]. Goldfarb, A. &. ((2011)). Online Display Advertising: Targeting and Obtrusiveness. Marketing Science, 30(3), 389–404. Retrieved from <https://doi.org/10.1287/mksc.1100.0583>
- [48]. Granados, N. G. ((2008)). Online strategies for the information age: Information transparency as a dimension of information systems design. . Info. Sys. Res.
- [49]. Gupta, R. P. ((2020).). Cyber security assessment education for E- governance systems. In K. Daimi, & G. Francia, III (Eds.), Innovations in Cybersecurity education. Cham: Springer.
- [50]. Hair, J. B. ((2010).). Multivariate Data Analysis. (7th Ed.). Prentice-Hall, Englewood Cliffs.
- [51]. Hayes, A. ((2009)). Beyond Baron and Kenny: Statistical Mediation Analysis in the New Millennium.. Communication Monographs, 76:4, 408-420. doi., DOI: 10.1080/03637750903310360.
- [52]. Hayes, A. F. ((2018)). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach (2nd ed.). New York, NY: Guilford Press.
- [53]. Hayes, A. F. (2018). Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach. New York, NY: The Guilford Press. Journal of Educational Measurement, 51(3), 335–337. Portico. <https://doi.org/10.1111/jedm.1205>
- [54]. Hoffmann, C. L. ((2016).). Privacy cynicism: a new approach to the privacy paradox. . Cyber psychology: J. Psych. Res. Cyberspace 10(4), 1–18.
- [55]. Holbert, R. L. ((2020).). Conceptualizing, organizing, and positing moderation in communication research. . Communication Theory, 30(3), 227–246. Retrieved from . <https://doi.org/10.1093/ct/qtz006>
- [56]. Hui, T. K. ((2007)). Tourists' satisfaction, recommendation and revisiting Singapore. Tourism Management, 28(4), 965–975. Retrieved from <https://doi.org/10.1016/j.tourman.2006.08.008>

- [57]. Ibrahim, M. A. ((2015)). Adoption of ERP systems: Does information transparency matter? . *Telematics and Informatics*, 32(2), 300–310.
- [58]. Jaccard, J. ((2001).). Interaction effects in logistic regression (Vol. 135). Thousand Oakes,. CA: Sage.
- [59]. Jin, L. ((2022)). Review of Research on the Privacy Protection Behavior of Social Network Users. Proceedings of the 2021 International Conference on Social Development and Media Communication (SDMC 2021). Retrieved from <https://doi.org/10.2991/assehr.k.220105.119>
- [60]. Judd, C. M. ((1981).). Estimating the effects of social interventions. Cambridge, England: . Cambridge University Press.
- [61]. Kaiser, H. ((1970).). A second-generation little jiffy. . *Psychometrika*, Springer, 35(4) 401-415.
- [62]. Kaiser, H. F. ((1960).). The application of electronic computers to factor analysis. . *Educational and Psychological Measurement*, 20, 141–151.
- [63]. Kenny, D. A. ((1998).). Data analysis in social psychology. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.).
- [64]. Khan, K. K. ((2011).). Systematic reviews to support evidence-based medicine,. CRC Press. Retrieved from <https://doi.org/10.1201/b13411>
- [65]. Kim, D. P. ((2019).). Willingness to provide personal information: Perspective of privacy calculus in IoT services. . *Computers in Human Behavior*, 92, 273–281.
- [66]. Kim, D. P. ((2019).). Willingness to provide personal information: Perspective of privacy calculus in IoT services. . *Computers in Human Behavior*, 92, 273–281.
- [67]. Kim, D. P.-H. ((2019)). Willingness to provide personal information: Perspective of privacy calculus in IoT services. . *Computers in Human Behavior*, 92, 273–281.
- [68]. Kokolakis, S. ((2017)). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. Retrieved from <https://doi.org/10.1016/j.cose.2015.07.002>.
- [69]. Kopalle, P. K. ((2021).). EXPRESS: Big data, marketing analytics, and public policy: Implications for health care. . *Journal of Public Policy & Marketing*, 0743915621999031,453–456.
- [70]. Kotler, P. & ((2015).). .Principles of Marketing. Pearson.
- [71]. Lee, J. K. ((2017).). The effects of consumers’ Perceived Privacy Control on Perceived Privacy Risk in Location-Based Services. *International Journal of Contents*, Vol.13, No.1 .
- [72]. Lee, S. K. ((2017)). The effects of news consumption via social media and news information overload on perceptions of journalistic norms and practices. . *Computers in Human Behavior*, 75, 254–263. Retrieved from <https://doi.org/10.1016/j.chb.2017.03.013>
- [73]. Lee, Y. &. ((2009)). Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software. . *European Journal of Information Systems*, 18(2), 177–187. Retrieved from <https://doi.org/10.1057/ejis.2009.11>
- [74]. Lee, Y. &. ((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. .
- [75]. Li, Y. C.-J. ((2017)). PrivacyStreams. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1(3), 1–26. Retrieved from <https://doi.org/10.1145/3130941>
- [76]. Litt, E. ((2012)). Knock, Knock. Who’s There? The Imagined Audience. *Journal of Broadcasting & Electronic Media*, 56(3), 330–345. Retrieved from <https://doi.org/10.1080/08838151.2012.705195>
- [77]. Lutz, C., Hoffmann, C., & Ranzini, G. ((2020).). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media Soc.* 22, 1168–1187.
- [78]. M., C. (2000). Web surveys: a review of issues and approaches. . *Public Opin Q.* Winter;64(4):464-94. PMID: 11171027.
- [79]. Malhorta, 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).
- [80]. Martin, A. J. ((2017)). Motivation and engagement: Same or different? Does it matter? *Learning and Individual Differences*,. Retrieved from <https://doi.org/10.1016/j.lindif.2017.03.013>
- [81]. Martin, K. D. ((2017).). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. Retrieved from <https://doi.org/10.1007/s11747-016-0495-4>
- [82]. Mendenhall, M. E. ((2003)). Seeing the elephant: Human resource management challenges in the age of globalization. *Organizational Dynamics*, 32(3), 261-274.
- [83]. Moon, Y. ((2000).). Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers. *Journal of Consumer Research*, 26(4), 323–339. Retrieved from <https://doi.org/10.1086/209566>
- [84]. Mousavizadeh, M. K. (2016). Effects of assurance mechanisms and consumer concerns on online purchase decisions: An empirical study. *Decision Support Systems*, 92, 79–90. Retrieved from <https://doi.org/10.1016/j.dss.2016.09.011>
- [85]. Mutimukwe, C. K. ((2019)). Information privacy practices in E-government in an African least developing country, Rwanda. *Electronic Journal of Information Systems in Developing Countries*, 85(2). Retrieved from <https://doi.org/10.1002/isd2.120>
- [86]. Obi, T. ((2015)). Waseda University- IAC international government ranking survey, . research report of the Waseda University Institute of e-government, 2015.
- [87]. Pavlou, P. A. ((2007)). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 31(1), 105–136.
- [88]. Petronio & wesley t.Durham. (2008). *The International Encyclopedia of Interpersonal Communication*. International Encyclopedias of Communication.
- [89]. Petronio, S. ((2013).). Brief status report on communication privacy management theory. . *Journal of Family Communication*, 13(1), 6–14. Retrieved from doi:10.1080/15267431.2013.743426
- [90]. Petronio, S. &. ((2020)). Conceptualization and operationalization: utility of communication privacy management theory. *Current Opinion in Psychology*, 31, 76–82. Retrieved from <https://doi.org/10.1016/j.copsyc.2019.08.009>
- [91]. Petronio, S. &. ((2020).). Conceptualization and operationalization: utility of communication privacy management theory. *Current opinion in psychology*, 31, 76-82 .
- [92]. Petronio, S. ((2002).). Boundaries of Privacy: Dialectics of Disclosure. Retrieved from <https://doi.org/10.1353/book4588>
- [93]. Quach, S. T. ((2022)). Digital technologies: tensions in privacy and data. . *Journal of the Academy of Marketing Science*, available.
- [94]. Razi, A., Agha, Z., Chatlani, N., & Wisniewski, P. ((2020).). Privacy Challenges for Adolescents as a Vulnerable Population. . In Proceedings of the Networked Privacy Workshop of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 2.
- [95]. 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.
- [96]. Research methods for business students. (.5th ed., Pearson Education Limited).
- [97]. S, P. (2002).). *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.
- [98]. Saunders, P. L. ((2014).). Research Methods for Students. Erasmus University. Retrieved from ISBN, 1783762322, 9781783762323.

- [99]. Segijn, C. M. (2020). Perceptions of techniques used to personalize messages across media in real time. *Cyberpsychology Behavior and Social Networking*, 23(5), 329–337. Retrieved from <https://doi.org/10.1089/cyber.2019.0682>
- [100]. Solove, D. J. (2012). Privacy Self-Management and the Consent Dilemma. 126 *Harvard Law Review* 1880 (2013), GWU Legal Studies Research Paper No. 2012-141, GWU Law School Public Law Research Paper No. 2012-141, .
- [101]. Stone, E. F. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), 459–468. Retrieved from <https://doi.org/10.1037/0021-9010.68.3.459>
- [102]. Thompson, R. C. (1999). Organizational change: An assessment of trust and cynicism. US Department of Transportation: Federal Aviation Administration.
- [103]. Tucker, C. (2011). Social Networks, Personalized Advertising, and Privacy Controls. *SSRN Electronic Journal*. Retrieved from <https://doi.org/10.2139/ssrn.1694319>
- [104]. 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. Retrieved from <https://doi.org/10.1016/j.chb.2014.11.076>
- [105]. Vitak, J. (2012). The Impact of Context Collapse and Privacy on Social Network Site Disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451–470. Retrieved from <https://doi.org/10.1080/08838151.2012.732140>
- [106]. Walgrave, S. a. (2011). Selection and Response Bias in Protest Surveys. *Mobilization: An International Quarterly* 16(2):203–22. Retrieved from <https://doi.org/10.17813/mai.16.2.j475m8627u4u8177>
- [107]. Wang, W. Q. (2016). Effects of rational and social appeals of online recommendation agents on cognition- and affect-based trust. *Decision Support System*, 86(2016), 48–60.
- [108]. Weisburd, D. H. (2019). Updated protocol: The effects of problem-oriented policing on crime and disorder: An updated systematic review. *Campbell Systematic Reviews*. Retrieved from <https://doi.org/10.1002/cl2.1005>
- [109]. Welman, C. K. (2005). *Research Methodology*. (3rd ed.) Oxford University Press.
- [110]. Xu, H. (2007). The Effects of Self-Constraint and Perceived Control on Privacy Concerns. *International Conference on Interaction Sciences*.
- [111]. Xu, J. B. (2014). The nature and consequences of trade-off transparency in the context of recommendation agents. *MIS Q.*, 38(2), 379–406.
- [112]. Xu, J. D. (2011). The effects of service and consumer product knowledge on online customer loyalty. *Journal of the Association for Information Systems*, 12 (11), 741–766.
- [113]. Xu, J. D. (2011). The effects of service and consumer product knowledge on online customer loyalty. *Journal of the Association for Information Systems*, 12 (11), 741–766.
- [114]. Zeng, F. C. (2020). Understanding the spillover effects of channel reward on observers’ commitment: The mediating role of envy. *Industrial Marketing Management*, 93, 650–660. Retrieved from <https://doi.org/10.1016/j.indmarman.2019.01.003>
- [115]. Zhang, X., Tian, X., & Han, Y. (2022). Influence of Privacy Fatigue of Social Media Users on Their Privacy Protection Disengagement Behavior—.
- [116]. Zhao, X. J. (2010). Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. *Journal of Consumer Research*, 37 (2), 197-206.
- [117]. Zhou, L. W. (2018). Perceived information transparency in B2C e-commerce: An empirical investigation. *Information & Management*, 55(7), 47–79.

Annex 1: Standard Regression Weights, CR, AVE, Cronbach α , and Communalities

			Estimate	AVE	CR	α	Comm. Ex
PC1	<---	PCont	.650	.526	.768	.703	.701
PC2	<---	PCont	.740				.768
PC3	<---	PCont	.78				.570
PT1	<---	PTur	.730	.509	.751	.704	.785
PT2	<---	PTur	.845				.643
PT3	<---	PTur	.530				.609
PIT1	<---	PITr	.562	.595	.851	.847	.612
PIT2	<---	PITr	.772				.710
PIT3	<---	PITr	.912				.827
PIT4	<---	PITr	.798				.732
PCc1	<---	Pcy	.919	.802	.924	.923	.883
PCc2	<---	Pcy	.930				.920
PCc3	<---	Pcy	.834				.933
IDPI1	<---	IDPInt	.798	.827	.934	.931	.883
IDPI2	<---	IDPInt	.953				.920
IDPI3	<---	IDPInt	.967				.933

Annex 2: Model 58 Hayes (2018) PROCESS Results

Run MATRIX procedure:

***** PROCESS Procedure for SPSS Version 3.5.3 *****

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
 Documentation available in Hayes (2018). www.guilford.com/p/hayes3

Model : 58
 Y : Av_IDPI
 X : Av_PT
 M : Av_PIT
 W : Av_PCc

Sample
 Size: 335

OUTCOME VARIABLE:
 Av_PIT

Model Summary						
	R	R-sq	MSE	F	df1	df2
P	.222	.049	1.163	5.709	3.000	331.000
	.001					

Model							
	coeff	se	t	p	LLCI	ULCI	
constant	6.242	.824	7.572	.000	4.621	7.864	
Av_PT	-.634	.176	-3.603	.000	-.979	-.288	
Av_PCc	-.891	.324	-2.748	.006	-1.528	-.253	
Int_1	.206	.068	3.037	.003	.073	.340	

Product terms key:
 Int_1 : Av_PT x Av_PCc

Test(s) of highest order unconditional interaction(s):					
	R2-chng	F	df1	df2	p
X*W	.027	9.226	1.000	331.000	.003

 Focal predict: Av_PT (X)
 Mod var: Av_PCc (W)

Conditional effects of the focal predictor at values of the moderator(s):

	Av_PCc	Effect	se	t	p	LLCI	ULCI
	1.002	-.427	.120	-3.558	.000	-.662	-.191
	2.483	-.121	.083	-1.457	.146	-.284	.042
	3.963	.185	.140	1.316	.189	-.091	.460

Data for visualizing the conditional effect of the focal predictor:
 Paste text below into a SPSS syntax window and execute to produce plot.

```

DATA LIST FREE/
  Av_PT      Av_PCC      Av_PIT      .
BEGIN DATA.
  3.711      1.002      3.766
  4.433      1.002      3.458
  5.000      1.002      3.216
  3.711      2.483      3.582
  4.433      2.483      3.494
  5.000      2.483      3.426
  3.711      3.963      3.397
  4.433      3.963      3.530
  5.000      3.963      3.635
END DATA.
GRAPH/SCATTERPLOT=
  Av_PT      WITH      Av_PIT      BY      Av_PCC      .

*****
OUTCOME VARIABLE:
  Av_IDPI

Model Summary
      R      R-sq      MSE      F      df1      df2
p      .417      .174      1.288      17.385      4.000      330.000
.000

Model
      coeff      se      t      p      LLCI      ULCI
constant      -1.157      .583      -1.984      .048      -2.304      -.010
Av_PT      .414      .088      4.705      .000      .241      .587
Av_PIT      .715      .102      7.000      .000      .514      .916
Av_PCC      .875      .127      6.865      .000      .624      1.126
Int_1      -.217      .033      -6.575      .000      -.281      -.152

Product terms key:
  Int_1      :      Av_PIT      x      Av_PCC

Test(s) of X by M interaction:
      F      df1      df2      p
      .231      1.000      329.000      .631

Test(s) of highest order unconditional interaction(s):
      R2-chng      F      df1      df2      p
M*W      .108      43.227      1.000      330.000      .000
-----
      Focal predict: Av_PIT      (M)
      Mod var: Av_PCC      (W)

Conditional effects of the focal predictor at values of the moderator(s):
      Av_PCC      Effect      se      t      p      LLCI
ULCI
      1.002      .498      .077      6.466      .000      .346
.649
      2.483      .177      .057      3.098      .002      .065
.289
      3.963      -.144      .073      -1.963      .050      -.288
.000

Data for visualizing the conditional effect of the focal predictor:

```

The Disparity Effects of Privacy Turbulence, Control, and Information Transparency on the ..

Paste text below into a SPSS syntax window and execute to produce plot.

```
DATA LIST FREE/
  Av_PIT      Av_PCc      Av_IDPI      .
BEGIN DATA.
  2.410      1.002      2.754
  3.511      1.002      3.302
  4.612      1.002      3.849
  2.410      2.483      3.276
  3.511      2.483      3.471
  4.612      2.483      3.666
  2.410      3.963      3.798
  3.511      3.963      3.640
  4.612      3.963      3.482
END DATA.
GRAPH/SCATTERPLOT=
  Av_PIT      WITH      Av_IDPI      BY      Av_PCc      .
***** DIRECT AND INDIRECT EFFECTS OF X ON Y *****
Direct effect of X on Y
  Effect      se      t      p      LLCI      ULCI
  .414      .088      4.705      .000      .241      .587
Conditional indirect effects of X on Y:
INDIRECT EFFECT:
  Av_PT      ->      Av_PIT      ->      Av_IDPI
      Av_PCc      Effect      BootSE      BootLLCI      BootULCI
      1.002      -.212      .061      -.343      -.103
      2.483      -.021      .017      -.056      .012
      3.963      -.027      .030      -.103      .014
---
***** ANALYSIS NOTES AND ERRORS *****
Level of confidence for all confidence intervals in output:
  95.0000
Number of bootstrap samples for percentile bootstrap confidence intervals:
  10000
W values in conditional tables are the mean and +/- SD from the mean.
----- END MATRIX -----
Run MATRIX procedure:
***** PROCESS Procedure for SPSS Version 3.5.3 *****
      Written by Andrew F. Hayes, Ph.D.      www.afhayes.com
      Documentation available in Hayes (2018). www.guilford.com/p/hayes3
*****
Model      : 58
Y      : Av_IDPI
X      : Av_PC
M      : Av_PIT
```

W : Av_PCc

Sample
Size: 335

OUTCOME VARIABLE:

Av_PIT

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.181	.033	1.183	3.724	3.000	331.000
	.012					

Model

	coeff	se	t	p	LLCI	ULCI
constant	3.786	.782	4.844	.000	2.248	5.323
Av_PC	-.095	.171	-.553	.581	-.432	.242
Av_PCc	-.320	.252	-1.272	.204	-.815	.175
Int_1	.088	.054	1.619	.106	-.019	.194

Product terms key:

Int_1 : Av_PC x Av_PCc

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.008	2.622	1.000	331.000	.106

Focal predict: Av_PC (X)
Mod var: Av_PCc (W)

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

DATA LIST FREE/

```
Av_PC Av_PCc Av_PIT .
BEGIN DATA.
3.444 1.002 3.441
4.259 1.002 3.435
5.000 1.002 3.430
3.444 2.483 3.414
4.259 2.483 3.514
5.000 2.483 3.604
3.444 3.963 3.387
4.259 3.963 3.592
5.000 3.963 3.779
```

END DATA.

GRAPH/SCATTERPLOT=

Av_PC WITH Av_PIT BY Av_PCc .

OUTCOME VARIABLE:

Av_IDPI

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.354	.125	1.364	11.805	4.000	330.000
	.000					

Model	coeff	se	t	p	LLCI	ULCI
constant	.392	.525	.746	.456	-.641	1.425
Av_PC	.125	.080	1.572	.117	-.032	.282
Av_PIT	.631	.103	6.107	.000	.428	.834
Av_PCc	.831	.131	6.324	.000	.573	1.090
Int_1	-.199	.034	-5.897	.000	-.266	-.133

Product terms key:

Int_1 : Av_PIT x Av_PCc

Test(s) of X by M interaction:

F	df1	df2	p
.080	1.000	329.000	.778

Test(s) of highest order unconditional interaction(s):

M*W	R2-chng	F	df1	df2	p
-----	.092	34.769	1.000	330.000	.000

Focal predict: Av_PIT (M)
Mod var: Av_PCc (W)

Conditional effects of the focal predictor at values of the moderator(s):

ULCI	Av_PCc	Effect	se	t	p	LLCI
.584	1.002	.431	.078	5.537	.000	.278
.252	2.483	.136	.059	2.319	.021	.021
.008	3.963	-.159	.076	-2.072	.039	-.309

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

DATA LIST FREE/

```
Av_PIT Av_PCc Av_IDPI .
BEGIN DATA.
2.410 1.002 2.798
3.511 1.002 3.272
4.612 1.002 3.747
2.410 2.483 3.318
3.511 2.483 3.468
4.612 2.483 3.618
2.410 3.963 3.838
3.511 3.963 3.663
4.612 3.963 3.489
END DATA.
```

GRAPH/SCATTERPLOT=

Av_PIT WITH Av_IDPI BY Av_PCc .

***** DIRECT AND INDIRECT EFFECTS OF X ON Y *****

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
.125	.080	1.572	.117	-.032	.282

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

Av_PC	->	Av_PIT	->	Av_IDPI	
Av_PCc		Effect	BootSE	BootLLCI	BootULCI
1.002		-.003	.057	-.112	.115
2.483		.017	.014	-.004	.050
3.963		-.040	.030	-.114	.000

***** ANALYSIS NOTES AND ERRORS *****

Level of confidence for all confidence intervals in output:
95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:
10000

W values in conditional tables are the mean and +/- SD from the mean.

----- END MATRIX -----