RESEARCH ARTICLE

Don't Get Ads, Get Even: The Effects of Prior Experiences with Targeted SNS Advertisements on Young Filipino Facebook Users' Intention to Self-disclose Information through Clicks on Facebook

Antonette Macey D. Alvarez, Reena Bianca M. Co, Karylle Gray de Castro, Sophia A. Fernandez, and Laura Sofia H. Perilla
University of the Philippines Diliman

ABSTRACT

The ambiguous processes of Social Networking Sites (SNSs), particularly Facebook, in personalizing targeted advertisements have caused privacy concerns. With the youth being Facebook's primary advertising audience in the Philippines, the study inquired how their privacy considerations impacted their interactions with targeted advertisements. This was guided by integrating the study's variables into Petronio's (2002) Communication Privacy Management Theory.

Accordingly, the study theorized that young Filipino Facebook users' prior experiences with targeted advertisements on SNSs—namely Negative Prior Experiences (NPE) and Positive Prior Experiences (PPE)—affect their online privacy disposition composed of General Privacy Concerns (GPC) with SNSs and Institutional Trust (IT) in Facebook as a data-collecting firm. The study then conceptualized that the shifts in privacy disposition would influence Click-Through Intention in targeted advertisements on Facebook. Thus, the study utilized secondary data from a one-shot online survey administered to a volunteer sample of 789 young Filipino Facebook users who had encountered at least one targeted advertisement on Facebook.

Both types of prior experiences were discovered to influence privacy disposition, albeit NPE was more impactful on both GPC and IT. However, there were differences in the associations between privacy disposition and Click-Through Intention between the two groups of respondents. Those who have clicked on targeted advertisements before intend to click again regardless of GPCs and with motivation of their IT, while those who have not will only click due to their GPCs but may click due to their IT. Thus, the study shows that those with more experience with targeted advertisements on Facebook are more likely to find personalization useful. Moreover, they are more likely to have perceived

PCS REVIEW | SERIES (2024) : 30 - 68

ISSN 2094-8328 | e-ISSN 2961-3426

trust-building cues for Facebook, similar to collectivists, who provide insight into Filipino privacy orientation. Hence, this study offers a snapshot of young Filipino Facebook users' targeted advertisement engagement and demonstrates their need for privacy management education.

Keywords: *Privacy, Prior Experiences, Young Filipino Facebook Users, Targeted Advertisements, Communication Privacy Management Theory*

Introduction

The development of information technology has caused the ubiquity of targeted advertising. Targeted advertising is defined as methods that deliver individually catered advertisements based on the website's content, user's location, browsing history, demographics, and other available information (Farahat & Bailey, 2012). The vast amount of information online demands the monetization of specific data to cultivate higher interest and purchase intention, which requires an intensive collection of users' data (Farahat & Bailey, 2012; Meta, 2023).

However, the shadowy processes implemented by Social Networking Sites (SNSs) to "capture, store, aggregate, redistribute, and use data from individual users" (Houghton & Joinson, 2010, p. 77) have caused privacy violations. These stem from the misalignment of privacy policies of SNSs, how SNSs extract data, and the privacy preferences of users (Banerjee et al., 2011). Facebook remains the foremost example of when SNSs invade user privacy to curate targeted advertisements to its users due to the Cambridge Analytica data breach, which extracted the raw data of 87 million Facebook profiles for Trump's campaign, causing increased doubt on privacy regarding targeted ads (Rotter, 2018). Recent developments in Facebook's data policy show that its framing only addresses the data collected and not its methods (Boatwright & White, 2020). This vagueness results in the behavioral dichotomy of Facebook users who either condemn targeted ads due to surveillance or expect an algorithmic system that orchestrates their desires and needs on the interface (Ruckenstein & Granroth, 2020).

Prior experiences may determine a user's behavior toward an ad, such as ad engagement and ad avoidance (Rosengren & Dahlén, 2015). Negative experiences, such as experiences of ads misleading, exaggerating, and leading to unbecoming sites, and even the expectation of negative experiences when engaging with ads are antecedents to ad avoidance (Kelly et al., 2010). Conversely, ad personalization likely generates positive experiences by offering users hedonic, informational, and economic benefits, leading to ad engagement (Youn & Kim, 2019). Accordingly, users' experiences may reflect on whether or not they click on targeted ads. Scholars discussed how users are aware that clicking on an ad online reveals their preferences to the data-collecting medium and thus engage with targeted ads accordingly (Wang et al., 2015), as it may increase ad personalization (Aguirre et al., 2015). As opposed to covert methods of gathering the users' data (e.g., online behaviors, preferences), clicking on ads can be seen as deliberate user action. If users perceive online links as unsafe privacy-wise, they may choose not to click these ads.

Facebook users willingly trade personal information for benefits (e.g., services, discounts), making it a profitable marketing approach (Strycharz et al., 2019). Notably, Filipino youth aged 18 to 24 in the Philippines are the primary advertising audience on Meta platforms (Statista, 2023a). High exposure to SNS ads increases the likelihood of youth ad engagement and disclosure of personal information. On Facebook, the youth has displayed limited involvement in negotiating privacy controls (De Wolf et al., 2014) and prioritized content personalization over data privacy (Alvarez et al., 2022). Despite being aware of potential privacy violations, they still engage with targeted ads on Facebook to get product information (Youn & Shin, 2019; Zarouali et al., 2018).

Research Focus

With all the implications of the nature of targeted ads on SNSs and the possibility of young Filipino Facebook users' receptiveness to targeted ads, the study inquires into how these users receive targeted ads as manifest through clicking in response to their privacy disposition determined by their experiences with targeted ads. Specifically, the study inquires: How does prior experience with targeted advertisements in SNSs influence young Filipino Facebook users' intention to click on Facebook-targeted advertisements?

To explore this question, the study is guided by the following objectives:

1. Determine the respondents' prior experience with targeted advertisements in SNSs regarding their:
    a. Negative experiences (NPEs) and
    b. Positive experiences (PPEs)
2. Identify the respondents:
    a. Level of General Privacy Concerns (GPCs) and
    b. Level of Institutional Trust (IT) in Facebook
3. Assess the extent to which:
    a. Negative experience with targeted advertisements in SNSs affects GPCs and IT on Facebook
    b. Positive experience with targeted advertisements in SNSs affects GPCs and IT on Facebook
    c. GPCs and IT in Facebook affect repeated online disclosure behaviors through click-through intention (CTI).

Moreover, this study would contribute to the Communication Privacy Management (CPM) theory by contextualizing the framework's hypotheses to Facebook users, targeted advertisements, and CTI. Furthermore, contemporary studies regarding privacy concerns focus on the aftereffects of consumer behavior

rather than on prior experiences and beliefs (Cho et al., 2010), illustrating a methodological gap and a new angle for assessment. Significantly, this study will validate whether privacy assessment affects a user's responses to targeted advertisements. Overall, the study will emphasize the relevance and urgency of scrutinizing engagement with targeted ads among young Facebook users and contribute crucial information that can aid young Filipino Facebook users to understand better ad management structures and provide relevant policy and societal stakeholders data on how Filipino youth assess privacy-related situations with Facebook-targeted ads.

Literature Review

Prior Experiences

Prior experiences result from past experiences linked with targeted maladaptive and adaptive responses (Floyd et al., 2000). Individuals form inferences, attitudes, and beliefs about the world by combining the results from prior experiences (Labor et al., 2015). As targeted ads simultaneously utilize SNS users' personal information to cater to their interests and collect more data after interacting with such, prior experiences may be a determining factor in the users' willingness to engage with ads (Rosengren & Dahlén, 2015), and affect future online disclosure behaviors.

Negative prior experiences (NPEs) are a consumer's past experiences that left them dissatisfied and wary of the marketer or the SNS (Yang & Liu, 2014). NPEs in the SNS context can be understood through the social contract theory (SCT)–wherein a social contract exists between the consumer and marketer when the consumer trades their personal information to the marketer for perks–as users are provided the best possible content in exchange for their information (Luo, 2002). They assume their data will be protected and used responsibly. However, when their information is mishandled, users anticipate risks to their information and will adjust their behavior accordingly. Users with NPEs with privacy disclosure tend to have no sense of control, increased pessimism, sensitivity to risk (Cho et al., 2010), and increased privacy concerns (Yang, 2013), while young users have had NPEs with ads due to ad clutter, ad irrelevance, too personal ads, and deceptive covert ads (Youn & Kim, 2019).

Conversely, positive prior experiences (PPEs) can affect a person's negotiation of the SNSs' perceived benefits by increasing their perceived controllability and reinforcing their optimistic bias (Cho et al., 2010). When users have positive experiences sharing their information, their belief in the positive aspects of the practice is backed by sentimental value, which underrates their vulnerability to risk when revealing information. Furthermore, users fluctuate in their perception

of benefits if the magnitude of the incentives is enough to warrant excusing the potential dangers. Online users may update their privacy appraisal depending on their prior experiences, thus adjusting their cognitions on what they perceive as beneficial features (Wu et al., 2023).

When users have more PPEs, they become susceptible to overestimating the potential benefits over the risk. Thus, when compromises to their privacy occur, they are indifferent and believe such instances are outliers (Cho et al., 2010). Conversely, users with more NPEs have been observed to tighten their benefits criteria and decrease their perceived value of disclosure necessary for the efficiency of SNS services (Wu et al., 2023), such as targeted ads. Features that were once beneficial for the user lose their value due to distrust. As such, we hypothesize:

H_1: The user's NPEs with targeted advertisements are negatively associated with the user's PPEs with targeted advertisements.

General Privacy Concerns

General privacy concerns (GPCs) are described as "an individual's general tendency to worry about information privacy" (Li et al., 2011, p. 5). In this context, users are concerned about the opportunistic behavior of SNSs as they disclose personal information online (Choi & Land, 2016). GPCs are part of online privacy disposition because they comprise individuals' privacy concerns across various SNSs (Xu et al., 2012).

GPCs may arise from prior negative encounters with targeted ads (Lina & Setiyanto, 2021). Moreover, the positive consequences of tailoring ads are weakened by feelings of intrusiveness at higher levels of privacy concern and negatively affect online consumers' purchase intentions (Van Doorn & Hoekstra, 2013). Thus, we hypothesize:

H_2: When the user's NPEs are more frequent than the user's PPEs, the user's NPEs are positively associated with the user's GPCs.

Contrastingly, positive experiences with targeted ads can reinforce the user's perception of the hedonistic value given by ads, subsequently reducing their perceived cost of the potential exchange of information and lessening avoidance (Youn & Kim, 2019). PPEs then reinforce the social contract between the user and the platform, as the benefits make the trade-off of getting ads more appealing. Moreover, Barbosa et al. (2021) found that users are reluctant to accept targeted ads due to privacy concerns. They are more open to them when consistent with their preferences, showing that benefits may repair privacy concerns. Given this, we hypothesize:

H_3: When the user's PPEs are more frequent than the user's NPEs, the user's PPEs are negatively associated with the user's GPCs.

Institutional Trust

Institutional trust (IT) in the information privacy context is the users' tendency to have confidence that data institutions such as SNSs will not mishandle their data in their pursuit to analyze personal data to improve user experience (Rosenthal et al., 2019). This is the users' assessment that SNSs will protect their information under rules of transaction conduct and privacy laws (Alsaleh et al., 2019). Hence, IT in Facebook is the users' expectation that Facebook will not exploit their data to act within public expectation (Rosenthal et al., 2019).

IT is the outcome of smaller interactions between individuals and the institution (Martin & Shilton, 2016). Therefore, prior experiences with targeted ads likely affect how users regard the trustworthiness of the SNSs. This can best be understood through SCT; users recognize that they exchange their personal information for free access to SNSs and personalization and assume this is handled responsibly (Rosenthal et al., 2019). Moreover, Rosenthal et al. (2019) observed this relationship in how PPEs with targeted ads improved institutional trust in Facebook—the more that users appreciated the personalization of targeted ads and subsequently tolerated data collection, the likelier it was that they were accepting of the SNS that provides them. As such,

H_4: When the user's PPEs are more frequent than the user's NPEs, the user's PPEs are positively associated with their IT.

Conversely, NPEs violate trust in data institutions providing targeted ads. Since users have social contracts with SNSs to guard their information, the contract is breached when they experience violations (Culnan, 1995). In the context of targeted ads, experiencing threats to information privacy is viewed as a violation of the social contract and thus decreases IT. Boerman et al. (2017) found that non-consensual collection and utilization of user information lowered trust in advertisers. Goles et al. (2009) further discovered that violations due to service failures by online marketers are attributed to the unreliability of the broader online market. This likely extends to SNSs that help deliver the ads as Yang and Liu (2014) found that negative experiences with online disclosure of information constitute breaches in the social contract between marketers and consumers, leading to lower trust in SNSs as they perceive that SNSs authorize what companies can do with personal information. With this, we hypothesize:

H_5: When the user's NPEs are more frequent than the user's PPEs, then the user's NPEs are negatively associated with the user's IT.

General Privacy Concerns and Institutional Trust

GPCs and IT are theorized to make up information privacy disposition, which affects perceptions of privacy online and influences disclosure (Kehr et

al., 2015; Rosenthal et al., 2019). Subsequently, GPCs and IT have been seen to have a negative relationship. Utility-wise, benefits enhance IT while privacy concerns lower IT, impacting their anticipated utility (Bansal et al., 2010, as cited by Rosenthal et al., 2019). In reference to SCT, users' trust in platforms is based on the data institutions' perceived responsibility in handling user data (Okazaki et al., 2009).

The negative relationship between GPCs and IT continues on Facebook. On Facebook, GPCs may act as emotions that attenuate trust, predisposing individuals to respond negatively to data collection by online firms, especially given Facebook's global privacy scandals (Rosenthal et al., 2019; Yang & Liu, 2014). Furthermore, Metzger (2006) found that Facebook users' privacy concerns negatively impact their trust in online companies and advertisers. Conversely, IT may influence perceptions of GPCs as addressing online privacy concerns can foster trust in online firms (Rifon et al., 2005), like Facebook, when their perceived integrity after data breaches helped increase IT (Ayaburi & Treku, 2020). Thus, it is hypothesized:

H_6: User's GPCs are negatively associated with the user's IT.

Click-Through Intention

Click-throughs–the act of clicking on online ads while having intentions to click-through (CTI)–are measured by the desire to directly engage with an advertising material by an action that will direct them to the advertised material (Yoo, 2009).

Yang and Wang (2009) posited that factors that intrude and meddle with information security negatively impact the intention to disclose, given that they elicit concerns that pertain to "information sensitivity… and the likelihood of information being sold to a third party" (p. 39). This is reflected in the way GPCs affect users' motivation to engage directly with targeted ads (Yang & Wang, 2009). Thus, it is hypothesized that:

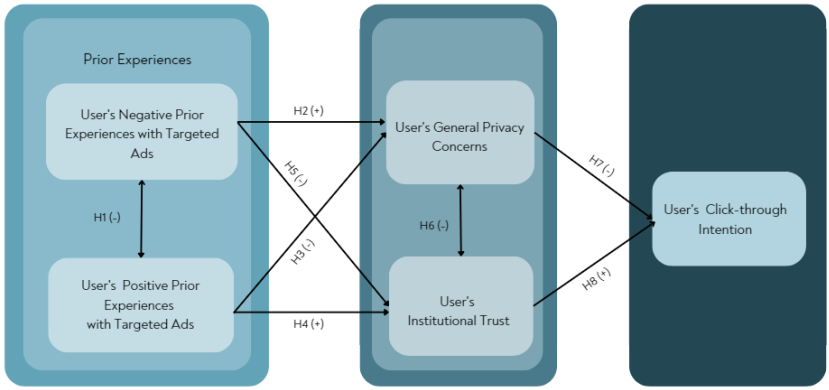
H_7: When the user's GPCs are higher than the user's IT, then the user's GPCs are negatively associated with the user's CTI.

However, it is also argued that behavioral intention to engage in disclosure can be increased if privacy concerns are diminished by the effects of trust (Luo, 2002). Accordingly, Aguirre et al. (2015) and Chang et al. (2017) found that the higher the level of Facebook users' IT, the likelier they are to continue to use Facebook despite concerns about their usage. As such, it can be hypothesized that:

H_8: When the user's IT is higher than the user's GPCs, the user's IT is negatively associated with the user's CTI.

Figure 1.

Hypothesis Pathing



The Filipino Context of Prior Experiences, Privacy Disposition, and Click-through Behaviors

The Filipino people's privacy protections are linked to their fundamental human rights. The Philippine government has taken steps to combat online abuse and misinformation through the Subscriber Identity Module (SIM) Card Registration Act (Morales, 2022) and cybercrime law to safeguard online spaces. Moreover, the National Privacy Commission has committed to fostering a strong culture of privacy and continuing its awareness campaign on the Data Privacy Act of 2012 (Dela Cruz, 2022), which is crucial as Filipinos are particularly vulnerable to cyber threats, phishing, and malware attacks (Omorog & Medina, 2017).

The nation's societal cohesion hinges on its online landscape's overall cyber safety and security. Consequently, there is a pressing need to address privacy violations within the media sphere. Measures to rectify these violations have become a top priority, reflecting the determination to uphold the privacy rights of Filipino citizens and create a safer digital environment for all.

Examining Filipinos' privacy landscape and online advertising approach, it is projected that the number of Facebook advertising users in the Philippines will reach 76.14 million by 2023 (Statista, 2023b). This substantial user base underscores the significance of continuous ad exposure, aligning with existing studies that delve into how Filipino users navigate their privacy preferences when interacting with SNS advertisements. This is even more worrying, considering that some Filipinos find online advertising beneficial despite personalization (Antonio et al., 2022; Araujo et al., 2022).

The most vulnerable here are the youth, who constitute a large percentage of social media users in the Philippines and with high social media usage. This is especially worrying in the context of Facebook as a platform that creates enticing personalized ads through dubious data collection practices because international findings illustrate that the youth rarely engage in privacy control on Facebook and may not have enough knowledge to understand the personalization and persuasion tactics that Facebook ads use (Arugay & Baquisal, 2022; Youn & Kim, 2019). Young Filipino users are also receptive to targeted ads and feel personalization enhances their online shopping experience (Antonio et al., 2022). It is imperative to investigate the connection between their experiences online, privacy disposition, and interactions with targeted advertisements.

Despite the glaring necessity to address the Filipinized culture of privacy management, little literature exists on how young Filipino users' experiences with SNSs have affected their interactions with Facebook-targeted ads. Thus, the study nuances this phenomenon to the local context through the salient literature it has garnered. As such, this study aims to remedy the localized literary gap that addresses the relationship between Filipino youth and Facebook-targeted ads via their experiences on SNSs.

The significance of previous experiences as cues and the existence of the privacy disposition in Filipinos is compelling in the literature. Filipinos have been seen to want to maintain privacy online (Mckay, 2010), and their experiences have acted as cues for their concern about information privacy and the level of trust in data institutions. Specifically, NPEs impact the information privacy concerns perceived by Filipino users, and PPEs contribute to how much they trust platforms (Doce & Celis, 2020; Capistrano, 2020). Albeit outside of the targeted advertising setting, these studies illustrate the relationship between Filipinos' prior experiences and privacy disposition.

Moreover, a weighty point for consideration is that the Philippines is a collectivist society (Church et al., 2012). Cultural differences influence how societies view privacy, differing between individualistic and collectivist cultures. On the one hand, individualistic cultures, which emphasize individualism and independence, focus on an individual's privacy management strategies, such as corrective and information control strategies, to protect one's online privacy (Li, 2022). On the other hand, collectivist cultures have been shown to account for the privacy of others and are cognizant of privacy risks for both themselves and the collective (Trepte et al., 2017). Additionally, James et al. (2017) found that members of collectivist nations are likely to use their Facebook privacy controls if there is a perceived risk of exposing others' information. However, the perceived risk of collectivists can be attenuated by trust in SNSs if their trust is fostered by cues signaling the benevolence of SNSs that signal the predictability of their

future actions (Krasnova et al., 2012). Overall, these findings entail that Filipino Facebook users can be expected to avoid targeted ads if they find them risky to themselves and others unless they can find trust-building cues from Facebook that demonstrate that the platform handles data in a trustworthy and reasonable manner.

However, an added consideration as to why young Filipino users may also interact with targeted ads is that they believe that personalization makes it easier for them to shop. In Antonio et al.'s study (2022), many young respondents were likely to purchase based on information from targeted ads due to the ease of shopping. This may indicate that they trust the SNSs enough to feel that there is no risk to them, only utility, reflecting the findings from Schumann et al. (2014). As companies have used click-throughs to measure engagement with targeted ads of Filipino youth, clicking intention could be relevant in checking whether or not young Filipino Facebook users find enough trusting cues or convenience in interacting with targeted ads to exceed their privacy concerns. Overall, there is evidence that Filipino users' experiences function as a basis for how they view privacy risks online and trust online platforms separately. However, the two interact to determine whether or not the users observe enough trusting cues to consider clicking. Thus, there is evidence that this phenomenon is present locally and that the variables identified are relevant to studying it.

Study Framework

The study investigated how prior experience with targeted ads on Facebook in SNSs influences Filipino youth Facebook users' privacy management as manifested through CTI. Accordingly, the theoretical framework of this study addressed its inquiry through two interrelated levels—macro and micro. On a macro level, the theory provided the system and general parameters by which young Filipino Facebook users regulate their CTI in response to their privacy disposition based on their prior experiences. However, a micro-level analysis is necessary to comprehend fully how these users undergo this process.

Macro-Level Analysis: Communication Privacy Management Theory by Petronio (2002)

Communication Privacy Management (CPM) theory explains how individuals actively manage private information through the creation of boundaries between the private (self) and public that determine the extent of their self-disclosure (Petronio, 2002). It illustrates how individuals identify their private information or the information they believe carries potential vulnerabilities and how they negotiate between the need to communicate it and

to preserve their freedom (Petronio, 2016).

Under CPM, ownership is represented by privacy boundaries that indicate how much personal information will be disclosed (Petronio & Child, 2020). Two levels of ownership exist: (1) the individual level involves sole ownership over private information, and (2) the information is shared with other parties or co-owners, and the privacy rules are co-constructed (Petronio, 2016).

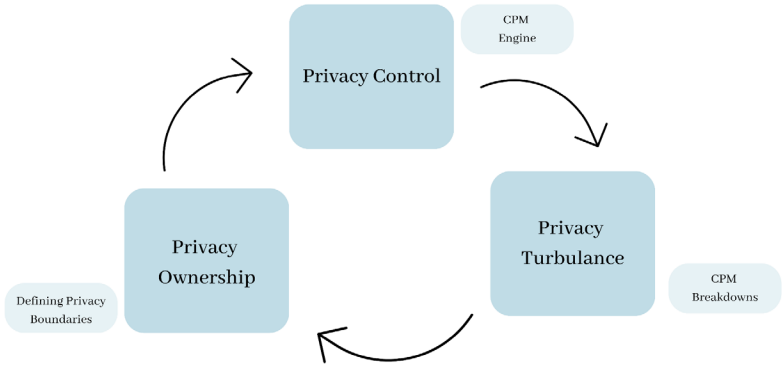
CPM has three operating principles for comprehending everyday privacy management (Petronio & Child, 2020). First, the process of creating private information ownership boundaries encompasses the shifting of ownership boundaries (Xie & Karan, 2019). This means that when an individual discloses information, it shifts from their boundary to a mutual boundary (Petronio, 2002). Second, private information control rules involve the development of privacy rules formed through personal experience. These criteria help regulate ownership boundaries and control disclosure in varying situations (Petronio & Child, 2020; Xie & Karan, 2019). When this process occurs for a mutually held boundary, the owner expects how the co-owners should treat their information, and they ideally coordinate privacy rules. Third, privacy information turbulence involves renegotiating privacy rules due to the violation or ambiguity of rules (Petronio, 2016). Turbulence may stem from minor infractions to significant infringements. This can be triggered by co-owners violating privacy rules or potential co-owners who may not be held accountable by an explicit agreement. This signals the need for change in the privacy management system regarding privacy rules, boundaries, control, and others (Petronio & Child, 2020).

CPM has recently been employed to investigate privacy management on SNSs, and this has yielded findings that users manage their privacy with advertisers or platforms as co-owners (Jacobson et al., 2020; Xie & Karan, 2019). [Figure 2].

Micro-Level Analysis

The micro-level follows the parameters set by the theory and nuances the theory to the phenomenon being studied. The following assumptions underpinning the theoretical proposal illustrate the interrelationship between the macro and micro levels: (1) in this context, Facebook functions as the co-owner of private information; (2) prior experiences with targeted ads on SNSs are the basis of Facebook users' online privacy rules with negative experiences operating as privacy information turbulence and positive experiences functioning as signals that it is safe to maintain or open boundaries; (3) general privacy concerns and institutional trust comprise online privacy rules that Facebook users consider when deciding whether or not to click; (4) clicking on targeted ads on Facebook is a disclosure behavior that reveals private information.

Figure 2.
Communication Privacy Management Model



First, Facebook may act as a co-owner of private online information because it is the party that Facebook users acknowledge they have to "coordinate" with to ensure that their private information is being shared and utilized in a manner they deem responsible. In the Facebook context, users see the platform as a co-owner of the information they disclose due to its well-known access to user information and its encouraging users to view the platform as an entity (Zhu & Kanjanamekanant, 2021). Specifically, Facebook is likely perceived as a co-owner of the preferences they reveal through their interactions with targeted ads on the platform, as it is well-established that Facebook gathers this data.

Second, prior experiences with SNSs serve as a factor that can catalyze change in and develop Facebook users' privacy rules. In general, prior experiences function as heuristics users rely on when assessing personal vulnerability when disclosing information online (Xie & Karan, 2019). In the context of targeted ads, the type of experience most frequently sustained by a user can lead to the readjusting of privacy rules because users connect their experiences with targeted ads with the state of information privacy and the decisions of online platforms (Xie & Karan, 2019). Users may presume that their experiences in the online ecosystem will likely be reflected in their experiences on a platform, particularly their experiences on SNSs, which affect their privacy management on Facebook. Specifically, NPEs on SNSs can act as privacy turbulence that leads to boundary tightening, causing an increase in online privacy concerns and decreasing trust in Facebook as a privacy co-owner. In contrast, PPEs on SNSs may prompt the user's boundary to be maintained or opened, lowering online privacy concerns and increasing trust in Facebook (Xie & Karan, 2019). Prior experiences may be weighed against each other and affect users' privacy rules.

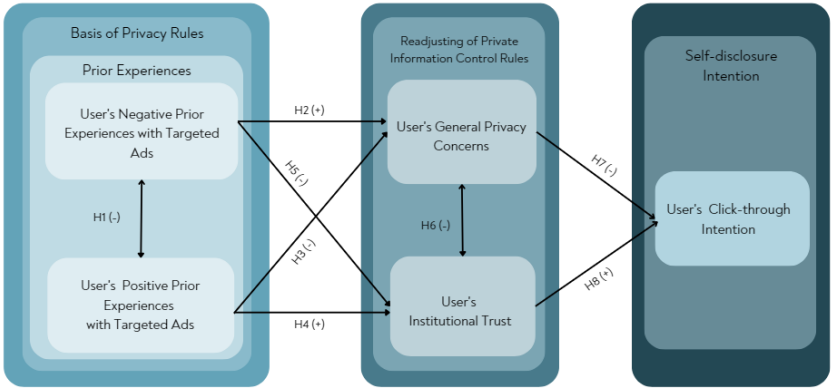
Third, GPCs and IT are the privacy rules that accommodate the shifting privacy boundaries of users. In this context, GPCs and IT comprise information privacy disposition, which users consider when regulating online disclosure (Kehr et al., 2015; Chang et al., 2017; Rosenthal et al., 2019). Furthermore, the current study argues that these rules are weighed against each other because they both influence users' tendency to have confidence in authorizing data-collecting institutions to be co-owners of private information through disclosure (Kehr et al., 2015; Petronio, 2016). Specifically, GPCs cause users to protect their private information online because they worry that disclosing could expose them to risks. IT allows users to share their private information online since they feel that the specific data-collecting institution they are directly disclosing to will not expose them to such risks.

Fourth, clicking is the disclosure act that manifests the privacy management of Facebook users regarding targeted ads because users primarily regulate their clicks, being aware that they signal interests to advertisers (Boerman et al., 2017). Moreover, some research argues that users perceive their preferences as private information, and clicking on ads is an act of being vulnerable to such data (Boerman et al., 2017). Consequently, clicking responds directly to the privacy rules as it has been found to react to privacy concerns and trust in advertisers (Boerman et al., 2017). Hence, CTI is an apt measure of how Facebook users will manage the disclosure of their preferences when interacting with targeted ads.

Under the CPM theory, the phenomenon can be explained as a result of prior experiences with SNSs, which cause changes in privacy boundaries that shift online privacy rules and thus impact clicking intention on targeted ads on Facebook. Overall, the privacy management process of young Filipino Facebook users can be said to follow the CPM theory.

Figure 3.

Integration of CPM and Micro-Analysis Model



Methodology

The study is exploratory because it investigates how experiences with targeted ads on SNSs affect the CTI of Filipino youth users toward the targeted ads they see on Facebook through their information privacy disposition. The study uses secondary data from the authors' study of young Filipino users' privacy disposition and its influence on the privacy risk-benefit calculus to assess Facebook targeted ads and their responding CTI. Subsequently, the study is implemented through the quantitative method of a one-shot online survey administered over three months.

The 53-item survey administered was composed of six sections that inquired about the respondents' (a) demographic characteristics, (b) experiences with targeted ads on SNSs, (c) targeted ad exposure and Facebook usage, (d) GPCs, (e) IT, and (f) CTI. Relevantly, prior experiences were measured on a five-point Likert scale (1 = "never," 5 = "always"), while GPCs, IT, and CTI were measured on a different five-point Likert scale (1 = "strongly disagree," 5 = "strongly agree").

Concepts, Dimensions, and Indicators

Young Filipino Facebook users' **negative prior experience** comprise the risks they feel they have been exposed to from interacting with Facebook-targeted ads. They are the user's suspicions that Facebook has compromised their data to facilitate targeted advertising and are measured through (1) invasiveness and (2) intrusiveness. Invasiveness is the user's perception that some entity or practice violates privacy (Gironda & Koraonkar, 2018). Intrusiveness is the interruption of a user's cognitive activity through forced exposure to ads, prompting feelings of loss of control (Youn & Shin, 2019).

Young Filipino Facebook users' **positive prior experiences** comprise the benefits they feel they have gained from interacting with Facebook-targeted ads. They are the users' assessment of the value of the personalized product information from Facebook targeted advertising, measured through (1) perceived ad value and (2) perceived personalization. Perceived ad value is the users' expected benefits–namely general informativeness, entertainment, and promotional reward–from trading their personal information, which helps make Facebook ads attractive and less intrusive (Youn & Shin, 2019). Perceived personalization is the degree to which a user senses an ad has been personalized to them and that it is relevant to their preferences and interests (de Groot, 2022).

Young Filipino Facebook users' **general privacy concern** refers to their tendency to worry about their information privacy on SNSs. It is the user's apprehension about the information collection and use of SNSs (Zarouali et al., 2018). Three constructs by Malhotra et al. (2004) encompass this: (1) awareness

of privacy practices, (2) concern for data collection, and (3) concern for data control. The first is the level at which users are worried about their awareness of organizational information privacy practices. The second is triggered by online companies asking for personal information and encompasses the extent to which the user is disturbed by the ways they may misuse such. The third comprises users' worries about their level of control over personal data through platform affordances.

Young Filipino Facebook users' **institutional trust** refers to their general tendency to have confidence in Facebook or how much they trust Facebook to protect their data. Trusting beliefs can further explain the degree to which users believe a firm will protect their information (Malhotra et al., 2004).

The young Filipino Facebook user's **click-through intention** refers to their intent to click on a targeted Facebook ad to see its material, a manifestation of their interest. This unidimensional concept measures the intention to click on a personalized ad scale (Gironda & Korgaonkar, 2018) [Table 1].

Each scale that made up the final survey and its items can be found in Appendix A.

The survey was administered online to respondents who were (a) of Filipino nationality, (b) 18-24 years old, (c) Facebook users, and (d) exposed to at least one (1) targeted ad on Facebook. The survey was distributed via Google Forms on Facebook and Instagram to a volunteer sample of 923 respondents. After cleaning the dataset, the study retained 789 valid respondents.

Table 1.

Prior experiences with SNSs' targeted advertisements measures

Variable	Measure		Source
Prior experiences with SNSs' targeted advertisements	Negative prior experience ● Experienced risks	Experienced invasiveness	Gironda & Korgaonkar, 2018
		Experienced intrusiveness	Youn & Shin, 2019
	Positive prior experience ● Experienced benefits	Experienced ad value	
		Experienced personalization	de Groot, 2022

Variable	Measure	Source
GPC	Awareness of privacy practices	Malhotra et al., 2004
	Concern for data collection	
	Concern for data control	
IT	Trusting beliefs	
CTI	Click-through reasons	Gironda & Korgaonkar, 2018

Validity and Reliability Testing

Reliability was assessed using Cronbach's alpha. The Cronbach's alpha of the questionnaire was 0.712, greater than the generally agreed upon lower benchmark of 0.70. This supports the reliability of the measurement scheme [Appendix B].

Discriminant validity was assessed using the Fornell-Larcker criterion (Fornell-Larcker, 1981). The results of the assessment supported the discriminant validity of the measurement scheme. However, the Fornell-Larcker criterion still needs to be met for two pairs of latent constructs, indicating that they measure the same concept. The items for experienced intrusiveness were not distinct from the items for experienced invasiveness (LEInv) since the AVE of LEIntru (0.573) is less than the correlation of LEIntru with LEInv (0.688). The two constitute NPEs. Similarly, the items for experienced ad value (LEAdVal) were not distinct from the item for experienced personalization (LEPrs) since the AVE of LEAdVal (0.549) was less than the correlation of LEAdVal with LEPrs (0.579) [Appendix C]. The two comprise PPEs.

Data Analysis

The demographic composition of the sample was summarized using the appropriate measures of central tendency. Given their interval nature, the exposure variable and study variables were summarized using the measure of mean.

Although the study's sample is non-parametric, the researchers tested the associations at the interval level and applied linear regression (R) to establish causation. However, the significance level (p) is not reported as the study limits its discussion to the sample and does not generalize to the population. Accordingly, Spearman's rho statistical tests (rs) were utilized between the following pairs of variables: (1) NPEs and PPEs, (2) NPEs and GPCs, (3) PPEs and GPCs, (4) PPEs and IT, (5) NPEs and IT, (6) GPCs and IT, (7) GPCs and CTI, (8) IT and CTI.

Furthermore, to address the hypotheses, the respondents were categorized based on their prior experiences: those with NPEs and those with PPEs. This was done by computing the mean value for both types of experience. Consequently, the higher mean for each respondent represented their type of prior experience. Moreover, the respondents were split into two groups according to their CTI: those who have and have not clicked. Those who have not clicked are conceptually treated as a control group, as they have less basis for assessing how their data was used to create targeted ads than those who clicked.

Scope and Limitations

The sample of this study is non-parametric. Thus, its findings may only represent some of the entire population of Filipino Facebook youth users. Furthermore, while many CPM studies are implemented through surveys, the study's survey method is limited to establishing associations between variables (Gravetter & Wallnau, 2014). To narrow in on how the identified experiences impact privacy control rules that determine disclosure intention, the study did not further investigate the cyclical nature of CPM in terms of how more NPEs or PPEs could affect the shifted privacy boundaries and rules. This aligns with how CPM is operationalized, as many CPM studies analyze their selected phenomena by focusing on one or two CPM concepts (Petronio & Child, 2020).

Results and Discussion

The descriptive statistics results revealed that a majority of the respondents are young female undergraduates with a middle-class income. Moreover, they are often exposed to targeted advertisements and have negative experiences. The study found very weak to moderate associations between variables. The interpretation is presented accordingly in the discussion.

Overall, many of the respondents are 21 years old, and most are female. Moreover, most respondents have a monthly household income between PHP 30,080 to PHP 66,640. Furthermore, the majority of the respondents have achieved the status of college undergraduate as their highest educational attainment [Table 2].

Table 2.

Summary Statistics for Demographic Variables

Variables	Results
Age	M = 21, SD = 1.58
Sex assigned at birth	Mo = Female (2.00)

Variables	Results
Monthly household income	*Md* = Between PHP 30, 080 to PHP 66,640 (4.00)
Highest educational attainment	*Md* = College Undergraduate (5.00)

Respondents report that they often see targeted ads (M = 4.42, SD = 4.84). Respondents spend 3.08 hours (SD = 2.53) on Facebook. Accordingly, they see an average of 10 targeted ads on their timeline (M = 9.50, SD = 8.90) [Table 3].

Table 3.

Summary Statistics for Exposure Variables

Variables	Results	
	M	*SD*
Hours spent on Facebook	3.08	2.53
Frequency of seeing targeted ads	4.42	4.84
Amount of ads seen on the timeline	9.50	8.90

Respondents have more frequent NPEs than PPEs. Moreover, respondents are disposed to GPCs more than IT. Furthermore, respondents who have not clicked before show a higher intention to click on targeted ads than those who have clicked before [Table 4].

There is a weak negative association between the respondents' NPEs and PPEs (R = 0.11, B = -0.11), such that the more NPEs a respondent has, the fewer PPEs they have. This association can be explained about 11% of the time. Thus, H_1 is partially supported [Table 4].

Table 4.

Summary Statistics for Study's Variables

Variables	Results	
	M	*SD*
NPEs	3.48	0.73
PPEs	2.68	0.73
GPC	4.43	0.50
IT	2.35	0.85
CTI *(Have clicked before)*	3.31	0.51
CTI *(Have not clicked before)*	3.59	5.79

Regarding GPCs, there is a moderate positive association with the respondents' NPEs (R = 0.5, B = 0.34). Conversely, there is a very weak negative association with the respondents' PPEs (R = 0.10). Essentially, more NPEs increase GPCs, while more PPEs decrease GPCs. As such, GPCs can be predicted by NPEs 50% of the time and PPEs 10% of the time. Thus, H_2 and H_3 are supported, with partial support for H_3 [Table 5].

As for IT, there is a moderate positive association with the respondents' PPEs (R = 0.41, B = -0.48), whereas there is a weak negative association with the respondents' NPEs (R = 0.25, B = 0.30). Simply, more PPEs raise IT, and more NPEs lower IT. Subsequently, IT can be predicted by PPEs 41% of the time and NPEs 25% of the time. Thus, H_4 and H_5 are supported [Table 5].

There is a moderate negative association between the respondents' GPCs and IT (R = 0.36, B = -0.60), such that the more GPCs they have, the lesser their IT. This can be predicted 36% of the time. Thus, H_6 is supported [Table 5].

The two types of respondents differ regarding the association between GPCs and CTI. On the one hand, for respondents who have clicked before, there is a very weak positive association between their GPCs and CTI (R = 0.08, B = 0.08). On the other hand, for respondents who have clicked before, there is a very weak negative association between their GPCs and CTI (R = 0.05, B = -0.63). Thus, this means that for the respondents who have clicked before, when their GPCs increase, their CTI increases, while for the respondents who have not clicked before, this means that when their GPCs increase, their CTI decreases. These associations can be explained 8% and 5% of the time, respectively. Regarding the association between IT and CTI, the two types of respondents are. On one hand, for respondents who have clicked before, there is a weak positive association between their IT and CTI (R = 0.14, B = 0.09). On the other hand, for respondents who have clicked before, there is a very weak negative association between their IT and CTI (R = 0.04, B = 0.29). Thus, this means that for both types of respondents, when their IT increases, their CTI increases. These associations can be explained 8% and 5% of the time, respectively. On the one hand, for respondents who have clicked before, there is a very weak positive association between their GPCs and CTI (R = 0.08, B = 0.08). On the other hand, for respondents who have clicked before, there is a very weak negative association between their GPCs and CTI (R = 0.05, B = -0.63). Thus, H_7 and H_8 are partially supported [Table 5].

Table 5.

Summary Associations for NPE, PPE, GPC, IT, and CTI

Hypotheses	Association	*R*	*B*
H_1	*NPEs and PPEs*	*0.11*	*-0.11*
H_2	*NPEs and GPCs*	*0.5*	*0.34*
H_3	*PPEs and GPCs*	*0.10*	*-0.07*
H_4	*PPEs and IT*	*0.25*	*0.30*
H_5	*NPEs and IT*	*0.41*	*-0.48*
H_6	*GPCs and IT*	*0.36*	*-0.60*
H_7	*GPCs and CTI (Have clicked before)*	*0.08*	*0.08*
	GPCs and CTI (Have not clicked before)	*0.05*	*-0.63*
H_8	*IT and CTI (Have clicked before)*	*0.14*	*0.09*
	IT and CTI (Have not clicked before)	*0.04*	*0.29*

Experiences as a Basis of Privacy Rules

Accordingly, the study found a weak negative association between the two types of experiences and weak to moderate associations between experiences and GPCs and IT. This follows the management system set by CPM, which supports that personal experiences continuously shape an individual's privacy rules. This also validates that experiences on SNSs affect how users perceive their privacy on Facebook.

There was a weak negative association between the respondents' experiences that when NPEs are more frequent, PPEs are less frequent. This is supported by Yang and Liu's arguments (2014) that users are under the assumption that their disclosed information is protected under a social contract with the SNS until they are consciously subject to a privacy breach. Thus, NPEs increase cautiousness in divulging personal data in exchange because of their heightened sensitivity to risk, lessening the perception of personalized ad experiences as positive. Albeit weak, this shows that NPEs may have influenced the sample to become stringent in their criteria of benefits and their perceived value of disclosing to attain more accurate ads on SNSs (Wu et al., 2023).

Subsequently, the study's respondents were more likely to have NPEs than PPEs, which informed respondents in considering whether or not to disclose, corroborating the conceptualization of NPEs as privacy turbulence. Yang (2013)

reinforced this, finding that negative experiences are more psychologically impactful than beneficial use. Furthermore, this supports findings that the youth are also more likely to experience negative experiences due to increased ad clutter and perceived deceptive ads (Youn & Kim, 2019).

The Association Between Experiences and Privacy Disposition

This study found weak to moderate associations between prior experiences and privacy disposition. This confirms that NPEs act as privacy turbulence that greatly impacts privacy boundaries and rules, with negative experiences considered boundary turbulence.

Results suggest that the respondents' GPC increased with the number of NPEs they had. This finding can be illuminated under CPM, where NPEs were empirically found to amplify perceived risk and feed into stringent privacy control. Empirically, this supports previous findings that privacy violations result in elevated risk perceptions and privacy concerns in future online encounters (Lina & Setiyanto, 2021; Yang, 2013).

Conversely, the respondents' GPC decreased with the number of PPEs they had. This can be understood through CPM studies, which indicated how PPEs decrease risk perceptions and increase intent to disclose (Metzger, 2007; Xie & Karan, 2017). This aligns with findings that a social contract exists between the user and platforms (Luo, 2002) and that ad benefits could reinforce it by providing hedonistic value and accuracy (Barbosa et al., 2021; Youn & Kim, 2019).

There are also results that NPEs were negatively associated with the respondents' IT. This finding can be understood under CPM, where negative experiences were theorized to be perceived as violations of information privacy rules and lead to stricter boundary coordination with platforms as privacy co-owners. From the SCT perspective, this aligns with studies that found that users who have experienced breaches in their social contract are more likely to have lowered trust in data institutions (Boerman et al., 2017; Yang & Liu, 2014).

In turn, PPEs increased the respondents' IT. This is understandable through CPM, which indicates that PPEs may signal users to maintain or increase their IT as a co-owner of personal information (Yang & Liu, 2014). This aligns with Rosenthal et al.'s (2019) findings that the greater the utility in terms of relevance and tailoring that users experience from targeted ads, the greater their IT in Facebook's data collection practices.

The tests illustrated that NPEs yield a stronger association with GPCs and IT than PPEs. This indicates PPEs and NPEs inverse association, such that when users have more NPEs, they have fewer PPEs (Wu et al., 2023). As the study's respondents experienced more risks with SNSs' targeted ads, they likely

reconsidered the benefits they experienced from personalization. As a result, they become skeptical of their online privacy and attuned to the risks of online disclosure (Lina & Setiyanto, 2021) and lose trust in the security of the data institutions that hold it (Yang & Liu, 2014). Furthermore, these results indicate that the respondents were not simply receptive to personalization, as studies on Filipinos have identified (Antonio et al., 2022; Araujo et al., 2022). They also connected its utility to the trustworthiness of Facebook and its disutility to online privacy concerns (Doce & Celis, 2020; Capistrano, 2020). Thus, the sample is similar to that of youth internationally, whose experiences with targeted ads can alter their disclosure behaviors with personalization (Youn & Kim, 2019).

The Association Between Privacy Disposition and CTI

As the study theorized, the sample weighed their GPCs and IT as privacy rules to help them decide whether or not to click on targeted ads. The weighing of the two privacy rules manifests in the moderate negative association between the respondents' GPCs and IT. However, there were very weak to weak associations between the factors of online privacy disposition and CTI. Albeit exerting some influence on CTI, this illustrates that GPCs and IT are not the primary privacy rules users consider when deciding whether to click. Nonetheless, the respondents who had not clicked on targeted ads notably indicated that they would likely click due to their IT and not click due to their GPCs, aligning with the study's hypotheses.

The results which showed that GPCs and IT were weighed aligns with Rosenthal et al.'s (2019) study, which posited that trust in Facebook is inversely related to privacy concerns. However, as Facebook actively works to improve its trustworthiness, respondents may have considered the platform's desirable features, potentially reducing their GPCs (Ayaburi & Treku, 2020). This uniquely contributes to the knowledge that the sample weighs their GPCs and IT against each other, extending previous studies exploring how Filipinos experience one or the other (Capistrano, 2020; Doce & Celis, 2020).

Following CPM, the CTI in response to privacy disposition was posited to be the main disclosure intention when interacting with targeted advertising. The intention was theorized to be directed by privacy rules. Albeit the associations found were very weak to weak, this provided some support that users manage privacy in terms of targeted ads by regulating their clicks, especially for the respondents who have not clicked before.

The results for GPCs diverged between two types of respondents: those who have clicked on targeted ads on Facebook and those who have not. Specifically, the CTI of respondents who have clicked before was unexpectedly positively influenced by GPCs. This demonstrates that these respondents disregarded their

privacy concerns. This is in contrast to the factors in the literature that privacy invasion entirely negatively affects the intention to disclose and aligns with the findings that the youth interact with targeted ads despite privacy concerns (Yang & Wang, 2009). In contrast, the CTI of respondents who had not clicked before decreased when their GPCs increased. This could be elucidated by the findings of Youn & Kim (2019) that users who do not already have PPEs when interacting with targeted ads have a higher tendency to scrutinize the divulging of their personal information, demotivating them from interacting further. In this context, this indicates that the respondents who have not clicked before have GPCs that attenuate benefits they may have experienced. Thus, they see their preferences as private information not worth revealing and avoid clicking accordingly.

Moreover, Antonio et al. (2022) found that Filipinos view targeted ads as either privacy invasions or relevant. Apart from age, the current study's findings provide more context and show that previous clicking behavior may influence how one perceives targeted ads on Facebook.

For both respondents who have clicked before and those who have not, IT had a marginal positive influence on CTI, providing some evidence that Facebook's privacy policies, data management, and reputation serve as cues for the study's respondents that clicking on targeted ads is safe. Findings from Chang et al. (2017) that trust fostered by Facebook's functionality heightens continuance intention and Aguirre et al. (2015) that good perceptions of Facebook's reputation lead to CTI support this. Nevertheless, respondents who clicked before had a stronger association between their IT and CTI than those who did not. This suggests that those who have clicked before have more experience with Facebook and found more trust-building cues that exceed the negative experiences and concerns they have garnered from SNSs in general (Krasnova et al., 2012).

Overall, the respondents who have clicked before have a marginally higher CTI in response to their GPC and IT than those who have not. This could be explained by the findings of Xie and Karan (2019), who found that users who use online platforms for consumer purposes tend to disclose more on Facebook. Considering all of this, it is logical to view respondents who have clicked before as users who have had more experiences with the utility of targeted ads and that foster their trust in Facebook's data collection processes compared to the respondents who have not clicked before. The reason behind this is that clicking may have increasingly personalized targeted ads to the preferences of the users, making the ads and Facebook as a platform more enticing, thus keeping the respondents who have clicked before in a cycle of clicking.

Conclusion

This study examined young Filipino Facebook users' CTI for Facebook's targeted ads as informed by their privacy disposition as rules which is shifted by their experiences with SNSs' targeted ads. It found that the sample had more NPEs than PPEs with SNS's targeted ads. Thus, NPEs affected the respondents' privacy disposition greater than PPEs and resulted in a higher level of GPC. As such, NPEs increase GPC and decrease IT, whereas PPE does the opposite. However, the associations between PPE and privacy disposition are generally weaker. This sample's experiences of privacy violations in SNSs thus affected their perception of risk on Facebook. This is consistent with the analysis that the sample can weigh their concerns and perception of Facebook and contrasts some local literature that implied passive reception to personalization. Moreover, albeit the associations were very weak to weak, the respondents who have and have not clicked before differed in terms of the associations between their CTI and privacy disposition. Those who have clicked before will click regardless of their GPCs and with motivation of their IT. This confirmed that concerns may not thwart CTI. This can be linked with findings that trust may mitigate privacy concerns, especially for the youth. In the view of local literature, these users may also have more experience with the utility of targeted ads and the trust-building cues of Facebook, given their higher exposure. Those who have not clicked before will avoid clicking due to their GPCs and may click in the future due to their IT. This showed that these respondents may lack PPEs to reduce their GPCs due to their lack of experience, but may click if they find more cues to trust Facebook. Overall, results supported the hypotheses consistently, although some of the associations were weak.

Implications and Recommendations

Theoretical Implications and Recommendations

The study utilized CPM as a foundation for forwarding hypotheses about young Filipino users' privacy management on Facebook in response to their shifts in privacy rules due to various experiences with targeted ads on SNSs. Given the lacking literature on CPM and targeted advertising, the study shows that the theory is valuable for understanding the privacy management of interactions with targeted advertising and recognizes that users contend with SNSs as privacy co-owners. This extends CPM beyond interpersonal boundary coordination and fully reckons with the new norm of individuals negotiating with platforms through their privacy affordances. The results supported the idea that context experiences remain an essential basis for privacy management in

targeted ads. The study also uniquely contributes new privacy rules, GPCs and IT to contemplate. Despite weak associations with disclosure intention, their compelling connections with prior experiences with targeted ads demonstrate that users amass experiences in the wider SNS ecosystem and then link them with their information privacy concerns and assessments of individual SNSs. This provides a new look into how dynamic the privacy management of users is. Moreover, the divergent propensities to click among the respondents who have and have not clicked before exhibits the fluidity that various people exhibit in what they consider as private information. Furthermore, the study adds to literature on the mechanisms behind the online privacy management of young Filipino users. The study bolsters the viability of the theory to understand Filipino users whose privacy orientations have a basis in collectivism. Moreover, as CTI in response to IT was strongest for respondents who have clicked before, this affirms that trust-building cues remain important to the privacy management in the online context for collectivists like Filipinos. In summary, the study provides insight into how elements of the theory—experiences, privacy boundaries, and privacy rules—can explain how collectivists contend with their privacy needs in the context of the targeted ad.

Using CPM allowed for the macro- and micro-analysis of user behavior. It provided a sound framework for examining the phenomenon at hand. However, future research may investigate the cyclical aspect of CPM and investigate if additional negative or positive experiences could affect the already shifted privacy boundaries and rules to capture the entire dynamic process of privacy management that the theory has been designed to comprehend. Further, the very weak to weak associations between the privacy rules and CTI urge research into other variables that may affect CTI directly. Particularly, there is potential in examining how situation-specific risks and benefits may fit in CPM and interact with CTI given that the privacy calculus has been forwarded as one of the approaches to understanding engagement with targeted ads (Youn & Shin, 2019).

Methodological Implications and Recommendations

The study validates that the survey method is a productive method for implementing CPM even when extended to inquire about users' privacy management in terms of targeted ads. This is evidenced by the moderate reliability of the measurement scheme, showing that respondents understand the concepts in the survey consistently even as they are dealing with novel privacy concepts such as viewing Facebook as a privacy co-owner. Furthermore, methodologies in privacy concerns studies focus on the aftereffects of the consumer's behavior

rather than on the mechanisms backgrounding it, such as prior experiences and privacy dispositions (Cho et al., 2010).

The researchers recommend the exploration of the variables through experiment instead of the survey method which could have respondent-based errors. It would also make the usual parts of theorization under CPM tenable as it would allow analysis of what types of personal information the users would or would not disclose (Child et al., 2012) and whether or not additional negative and positive experiences can affect newly shifted boundaries and rules. Furthermore, the associations between privacy disposition and CTI were very weak to weak. Future research may look into adding other disclosure behaviors (e.g., likes, shares, comments, and others) to have multiple ways to gauge the effect of disposition on disclosure.

Practical Implications and Recommendations

The study provides implications for young Filipino users, policy-makers, and society. Although Facebook has prompted worry over their obscure data collection and targeted ad delivery processes, the platform has been garnering clicks from the youth due to their limited knowledge about personalization and persuasion tactics that targeted ads on Facebook leverage (Youn & Kim, 2019). The study's respondents who had clicked on targeted ads on Facebook before were susceptible to Facebook's enticement despite having GPCs, showing that they have inadequate know-how to manage their privacy needs and end up clicking on targeted ads due to their utility and good perception of Facebook. This reveals the reality that government policies and programs aiming for privacy protection have neglected properly equipping the youth who have been greatly exposed to targeted ads to address their GPCs.

Therefore, there could be more efforts by the government to ground privacy protection policies and educate young Filipino Facebook users on the importance of addressing their GPCs, even with disclosure behaviors that are as simple as clicking given SNSs' ambiguous data handling. Laws that incentivize better transparency measures from Facebook should be created, leading to a less invasive targeted ads delivery system and be a more ethical way for Facebook to realistically operate without heightening personalization, given that young Filipino users are likelier to click on ads when they perceive cues to trust Facebook. Safe and benefiting engagements fulfill social trust and mitigate concerns, enhancing ad reception and addressing privacy concerns regarding Facebook's ad data usage. Given the online environment where data are commodities and requirements in most aspects of online life (e.g., SIM Card Registration Act or SNS log-in credentials), it is pertinent to underscore the importance of privacy to disallow any institution from exploiting data for their interests.

References

Aguirre, E., Mahr, D., Grewal, D., Ruyter, K. d., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Alsaleh, D. A., Elliott, M. T., Fu, F. Q., & Thakur, R. (2019). Cross-cultural differences in the adoption of social media. *Journal of Research in Interactive Marketing, 13*(1), 119–140. https://doi.org/10.1108/JRIM-10-2017-0092

Alvarez, A., Co, R., De Castro, K., Fernandez, S. & Perilla, L. (2022). *Don't get ads, get even: The effects of prior experiences with targeted SNS advertisements on young Filipino Facebook users' intention to self-disclose information through clicks on Facebook* [Unpublished manuscript]. College of Mass Communication, University of the Philippines Diliman

Antonio, B., Jimenez, A., Dela Cruz, K. & Pantoja, E. (2022). Invasion or personalization: An overview on user attitudes towards the privacy issues in targeted advertising in NCR and its effect in consumer purchase behavior. *Journal of Business and Management Studies*, *4*(2). https://doi.org/10.32996/jbms.2022.4.2.4

Araujo, C., Perater, K., Quicho, A. & Etrata Jr., A. (2022). Influence of TikTok video advertisements on generation Z's behavior and purchase intention. *International Journal of Social and Management Studies*, *3*(2). https://ijosmas.org/index.php/ijosmas/article/view/123

Arugay, A. A., & Baquisal, J. K. A. (2022). Mobilized and polarized: Social media and disinformation narratives in the 2022 Philippine elections. *Pacific Affairs*, *95*(3), 549–573. https://doi.org/10.5509/2022953549

Ayaburi, E., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, *50*, 171–181. https://doi.org/10.1016/j.ijinfomgt.2019.05.014

Barbosa, N. M., Wang, G., Ur, B., & Wang, Y. (2021). Who am I? A design probe exploring real-time transparency about online and offline user profiling underlying targeted ads. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *5*(3), 1–32. https://doi.org/10.1145/3478122

Banerjee, M., Adl, R. K., Wu, L., & Barker, K. (2011). Quantifying Privacy Violations. In *Lecture Notes in Computer Science*. Springer Science+Business Media. https://doi.org/10.1007/978-3-642-23556-6_1

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Boatwright, B., & White, C. (2020). Is privacy dead? Does it matter? *Journal of Public Interest Communications*, *4*(1), 78. https://doi.org/10.32473/jpic.v4.i1.p78

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of advertising*, *46*(3), 363–376.

Capistrano, E. (2020). Determining e-Government trust: An information systems success model approach to the Philippines' Government Service Insurance System (GSIS), the Social Security System (SSS), and the Bureau of Internal Revenue (BIR). *Philippine Management Review*, *27*, 57–78. https://pmr.upd.edu.ph/index.php/pmr/article/view/342/341

Chang, S. E., Liu, A. Y., & Shen, W. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior*, pp. *69*, 207–217.

Child, J. T., Haridakis, P. M., & Petronio, S. (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. *Computers in Human Behavior*, 28(5), 1859–1872. https://doi:10.1016/j.chb.2012.05.004

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Choi, B. C.F., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Elsevier B.V.*, *53*(7), 868-877. https://doi.org/10.1016/j.im.2016.02.003

Church, A. T., Alvarez, J. M., Katigbak, M. S., Mastor, K. A.,Cabrera, H. F., Tanaka-Matsumi, J. & Buchanan, A. L.(2012). Self-concept consistency and short-term stability in eight cultures. *Journal of Research in Personality*,*46*(5), 556–570. doi:10.1016/j.jrp.2012.06.003

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*(2), 10–19. https://doi.org/10.1002/dir.4000090204

de Groot, J. I. M. (2022). The personalization paradox in Facebook advertising: The mediating effect of relevance on the personalization–brand attitude relationship and the moderating effect of intrusiveness. *Journal of Interactive Advertising*, *22*(1), 57–74.

Dela Cruz, R. C. (2022, June 10). NPC to create a 'strong culture of privacy' in PH. *Philippine News Agency*. https://www.pna.gov.ph/articles/1176392

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring Facebook's individual and group privacy management strategies. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03.010

Doce, L. J., & Celis, N. J. (2020). Understanding Filipinos' perceptions of data privacy in crowdfunding: A social contract and virtue theory perspective. *In Pacific Asia Conference on Information Systems* (p. 73). https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1072&context=pacis2020

Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03.010

Farahat, A., & Bailey, M. C. (2012). How effective is targeted advertising? *Proceedings of the 21st International Conference on World Wide Web*, 111–120. https://doi.org/10.1145/2187836.2187852

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*, 39–50

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. *Electronic Commerce Research and Applications*, *29*, 64–77. https://doi.org/10.1016/j.elerap.2018.03.007

Goles, T., Rao, S. V., Lee, S. M., & Warren, J. J. (2009). Trust violation in electronic commerce: customer concerns and reactions. *Journal of Computer Information Systems*, *49*(4), 1–9. https://doi.org/10.1080/08874417.2009.11645335

Gravetter, F. & Wallnau, L. (2013). Essentials of Statistics for the Behavioral Sciences. Cengage Learning.

Houghton, D. P., & Joinson, A. (2010). Privacy, social network sites, and social relations. *Journal of Technology in Human Services*, *28*(1–2), pp. 74–94. https://doi.org/10.1080/15228831003770775

Jacobson, J., Gruzd, A., & Hernández-García, Á. (2020). Social media marketing: Who is

watching the watchers? *Journal of Retailing and Consumer Services*, *53*, 101774. https://doi.org/10.1016/j.jretconser.2019.03.001

James, T. L., Wallace, L. G., Warkentin, M., Kim, B. C., & Collignon, S. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control

use. *Information & Management*, *54*(7), 851–865. https://doi.org/10.1016/j.im.2017.01.001

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Kelly, L. A., Kerr, G., & Drennan, J. (2010). Avoidance of advertising in social networking sites. *Journal of Interactive Advertising*, *10*(2), 16–27. https://doi.org/10.1080/15252019.2010.10722167

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering*, *4*(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Labor, J., Macasero, C., & Castelo, J. (2015). Is Entertainment the Key? Creativity and Emotional Engagement as Factors to Buying Behavior for Globe Tattoo's "Defy Expectation" TV Commercial. Journal of Communication Arts, 33 (2): 8-18. https://so02.tci-thaijo.org/index.php/jcomm/article/view/160332

Li, Y. (2022). Cross-cultural privacy differences. In B.P. Knijnenburg, X. Page, P. Wisniewski, H.R. Lipford, N. Proferes & J. Romano. (Eds.), *Modern socio-technical perspectives on privacy*. 267–292. Springer Cham. https://doi.org/10.1007/978-3-030-82786-1

Li, H., Sarathay, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support System, 51(3), 434–445. https://doi.org/10.1016/j.dss.2011.01.017

Lina, L., & Setiyanto, A. (2021). Privacy concerns in personalized advertising effectiveness on social media. *Sriwijaya International Journal of Dynamic Economics and Business*, *5*(2), 147-156. https://doi.org/10.29259/sijdeb.v5i2.147-156

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, *31*(2002), 111–118. https://doi.org/10.1016/S0019-8501(01)00182-1

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336–355. http://hdl.handle.net/1880/50264

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

McKay, D. (2010). On the face of Facebook: Historical images and personhood in Filipino social networking. *History and Anthropology*, *21*(4), 479–498. https://doi.org/10.1080/02757206.2010.522311

Meta. (2023). What is the Privacy Policy, and what does it cover?

Metzger, M. J. (2006). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00. https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Morales, N. (2022, February 3). *Philippines passes law to tackle anonymous social media abuse.* Reuters. https://www.reuters.com/world/asia-pacific/philippines-passes-law-tackle-anonymous-social-media-abuse-2022-02-03/

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising*, *38*(4), 63-77.

Omorog, C. D., & Medina, R. P. (2017). Internet security awareness of Filipinos: A survey paper. *International Journal of Computing Sciences Research*, *1*(4), 14-26. doi: 10.25147/ijcsr.2017.001.1.18.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* State University of New York Press.

Petronio, S. (2016). Communication privacy management. In K. B. Jensen, E. W. Rothenbuhler, J. D. Pooley, & R. T. Craig (Eds.), *The International Encyclopedia of Communication Theory and Philosophy* (1st ed., pp. 1–9). Wiley. https://doi.org/10.1002/9781118766804.wbiect138

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: utility of communication privacy management theory. *Current Opinion in Psychology*, pp. *31*, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339–362. https://doi.org/10.1111/j.1745-6606.2005.00018.x

Rosengren, S., & Dahlén, M. (2015). Exploring Advertising Equity: How a brand's past advertising may affect consumer willingness to approach its future ads. *Journal of Advertising*, *44*(1), 1–13. https://doi.org/10.1080/00913367.2014.961666

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A., & Ling, R. (2019). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology*. https://www.tandfonline.com/doi/full/10.1080/15213269.2019.1648218

Rotter, K. (2018, April 28). *Targeted ads: The good, the bad, the unavoidable. California Management Review Insights.* https://cmr.berkeley.edu/2018/04/facebook-ads/

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising, and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24. https://doi.org/10.1080/17530350.2019.1574866

Schumann, J. H., von Wangenheim, F., & Groene, N. (2014). Targeted online

advertising: Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing, 78*(1), 59–75. https//doi:10.1509/jm.11.0316

Statista. (2023a). *Meta's advertising audience Philippines 2023, by age and gender*. https://www.statista.com/statistics/1139168/philippines-social-media-advertising-audience-age-and-gender/

Statista. (2023b, August 16). *Number of users of facebook advertising in the Philippines 2018-2027*. https://www.statista.com/statistics/490455/number-of-philippines-facebook-users/

Strycharz, J., van Noort, G., Helberger, N., & Smit, E. (2019). Contrasting perspectives – practitioner's viewpoint on personalized marketing communication. *European Journal of Marketing, 53*(4), 635–660. https://doi.org/10.1108/EJM-11-2017-0896

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*, 3(1), 205630511668803. https://doi.org/10.1177/205630511668803

Van Doorn, J., & Hoekstra, J. C. (2013). Customization of online advertising: The role of intrusiveness. *Marketing Letters*, 24(4), 339–351. doi:10.1007/s11002-012-9222-1

Wang, W., Yang, L., Chen, Y., & Zhang, Q. (2015). A privacy-aware framework for targeted advertising. *Computer Networks*, *79*, 17–29. https://doi.org/10.1016/j.comnet.2014.12.017

Wu, D., Min, C., Le, Z., & Wang, Y. (2023). Vigilance and habituation: Polymorphic experience effects in internet users' privacy disclosure decisions. *Decision Support Systems*. https://doi.org/10.1016/j.dss.2023.113961

Xie, W., & Karan, K. (2019). Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students. *Journal of Interactive Advertising*, *19*(3), 187–201. https://doi.org/10.1080/15252019.2019.1651681

Xu, H., Teo, H.-H., Tan, B., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, *23*(4), 1342–1363. https://doi.org/10.1287/isre.1120.0416

Yang, H., & Liu, H. (2014). Prior negative experience of online disclosure, privacy concerns, and regulatory support in Chinese social media. *Chinese Journal of Communication*. https://doi.org/10.1080/17544750.2013.816756

Yang, H. (2013). Young American consumers' online privacy concerns, trust, risk, social media use, and regulatory support. *Journal of New Communications Research*, *5*(1), 1–30. https://jcsdcb.com/index.php/JCSDCB/article/view/123

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *The DATA BASE for Advances in Information Systems*, *40*(1), 38– 51. https://doi.org10.1145/1496930.1496937

Yoo, C. (2009). Effects beyond click-through: Incidental exposure to web advertising. *Journal of Marketing Communications*, *15*(4), 227–246. https://doi.org/10.1080/13527260802176419

Youn, S., & Kim, S. (2019). Newsfeed native advertising on Facebook: Young millennials' knowledge, pet peeves, reactance, and ad avoidance. *International Journal of Advertising*, *38*(5), 651–683. https://doi.org/10.1080/02650487.2019.1575109

Youn, S. & Shin, W. (2019). Teens' responses to Facebook news feed advertising: The effects of cognitive appraisal and social influence on privacy concerns and coping strategies. *Telematics and Informatics*, *pp. 38*, 30–45. https://doi.org/10.1016/j.tele.2019.02.001

Zarouali, B., Poles, K., Walrave, M., & Ponnet, K. (2018). The impact of regulatory focus on adolescents' evaluation of targeted advertising on social networking sites. *International Journal of Advertising*, *38*(2), 316-335. https://doi.org/10.1080/02650487.2017.1419416

Zhu, Y., & Kanjanamekanant, K. (2021). No trespassing: Exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media. *Information & Management*, *58*(2), 103314. https://doi.org/10.1016/j.im.2020.103314

About the Authors

ANTONETTE MACEY D. ALVAREZ is a Communication Research student from the University of the Philippines Diliman. She endeavors to understand inquiries regarding the effects of mass communication and interconnectivity.

REENA BIANCA M. CO is a Communication Research student from the University of the Philippines Diliman. She is interested in researching fandom, gender, and online behavioral studies.

KARYLLE GRAY DE CASTRO is a Communication Research student from the University of the Philippines Diliman. She is driven to pursue research inquiries on women and gender, children's welfare, and the realities of minority groups.

SOPHIA A. FERNANDEZ is a Communication Research student from the University of the Philippines Diliman. She conducts research into user experience, platform affordances, and reception of misinformation and disinformation.

LAURA SOFIA H. PERILLA is a Communication Research student from the University of the Philippines Diliman. Her interests in pop culture and online behavior, impression management, and women's studies reflect her feminist advocacy.

Appendix A: Fornell-Larcker Criterion Analysis of the First Order Constructs for the Assessment of Discriminant Validity

	EMLClkYN	EMLClkYY	EMLClkNN	EMLClkNY	LEInv	LEIntru	LEAdVal	LEPrs	LAwPrPr	LCDColl	LCDCont	LTrBe
EMLClkYN	0.703											
EMLClkYY	-0.321	0.712										
EMLClkNN	-0.013	-0.070	0.652									
EMLClkNY	0.022	0.119	-0.552	0.719								
LEInv	0.188	-0.134	0.181	-0.073	0.746							
LEIntru	0.246	-0.146	0.261	-0.085	0.688	0.573						
LEAdVal	-0.046	0.311	-0,057	0.130	-0.001	0.034	0.549					
LEPrs	-0.182	0.332	-0.130	0.149	-0.162	-0.160	0.579	0.804				
LAwPrPr	0.230	-0.162	0.160	-0.027	0.246	0.300	0.004	-0.058	0.789			
LCDColl	0.235	-0.136	0.171	-0.036	0.453	0.477	-0.042	-0.138	0.422	0.772		
LCDCont	0.197	-0.162	0.219	-0.083	0.386	0.393	-0.083	-0.164	0.479	0.637	0.753	
LTrBe	-0.089	0.226	-0.087	0.077	-0.405	-0.344	0.168	0.277	-0.164	-0.370	-0.392	0.901

Appendix B: Cronbach's Alpha Analysis of the Variable Items for the Assessment Reliability

	Construct	Items	Cronbach's alpha (α)
NPEs	Experienced invasiveness	Feelings of violation when seeing ads on SNSs	.714
		Feeling that my personal information has been accessed inappropriately by outside parties when I see targeted ads on SNSs.	.710
		Feeling that my personal information is being used without my knowledge for targeted ads on SNSs.	.712
	Experienced intrusiveness	Feeling unsafe when I see too many targeted ads while scrolling on SNSs	.707
		Feeling that targeted ads are obtrusive when using SNSs	.711
		Feeling discomfort with how my personal information is being used when seeing targeted ads that are too personalized on SNSs	.710
PPEs	Experienced ad value	Feeling that the use of personal information by SNSs makes their ads entertaining.	.700
		Feeling that the use of my personal information by SNSs makes their ads informative	.698
		Feeling that the use of my personal information is worth it when their ads offer free gifts and rewards.	.700
	Experienced Personalization	Feeling that the use of my personal information by SNSs for ads help me consider products that I want to buy.	.700
		Feeling that when SNSs use my personal information for ads, it gives me useful information about products that are relevant to me	.700
		Feeling that it is okay for SNSs to use my personal information as it is more convenient to see ads related to me than not	.706
		Feeling that the use of my personal information to customize ads will enhance my experience on SNSs.	.700

GPCs	Awareness of Privacy Practices	It is important to me that I understand which of my personal information is being gathered and collected by SNSs.	.710
		It is important that I understand what SNSs are doing with my personal information.	.709
		I am concerned about how SNSs use my personal information for their benefit.	.707
		I believe it is important to read and understand the privacy policies and terms of SNSs that I visit.	.708
	Concern for data collection	I feel that SNSs gather too much personal information from me.	.710
		I believe that SNSs are giving too much of my personal information to third-parties outside of the SNSs.	.709
		I feel that I have no control over what SNSs do with my personal information.	.713
	Concern for data control	I believe that SNSs do not secure and protect my personal information sufficiently.	.714
		I believe that SNSs should give more control to the user on what personal information is taken from them.	.711
IT	Trusting Beliefs	I find Facebook trustworthy in handling my personal information.	.705
		I trust Facebook because they provide privacy policies.	.703
		I trust Facebook with my personal information because of the completeness of the privacy policy they provide.	.702
		I trust that Facebook follows their Privacy Policies when handling my personal information.	.705
		I trust that Facebook keeps my best interests in mind when dealing with my personal information.	.702
		I trust Facebook with my personal information because others find the website trustworthy.	.704
		I find Facebook to be consistently honest with all users when it comes to using the personal information that I would provide.	.703
		I find that Facebook is consistent in keeping all users' information safe when they transact with the website.	.703

CTI of Those Who HAVE Clicked Before	Reasons to NOT click again	I do not intend to click on a targeted ad again because I feel my information will be collected.	.713
		I do not intend to click on a targeted ad again because I believe it would increase their volume and frequency on my timeline.	.712
		I do not intend to click on a targeted ad again because I feel my information will be vulnerable.	.709
		I do not intend to click on a targeted ad again because I feel that my purchases will be monitored.	.710
	Reasons to click again	I intend to click on a targeted ad again if I need the product, despite my privacy concerns.	.709
		I intend to click on a targeted ad again because they are an innovative and creative way of shopping.	.707
		I intend to click on a targeted ad again because they cater to my personal interests and needs.	.706
		I intend to click on targeted ads again because they improve my online shopping experience.	.703
CTI of Those Who HAVE NOT Clicked Before	Reasons to NOT click	I do not intend to click on a targeted ad because I feel my information will be collected.	.721
		I do not intend to click on a targeted ad because I believe it would increase their volume and frequency on my timeline.	.715
		I do not intend to click on a targeted ad because I feel my information will be vulnerable.	.716
		I do not intend to click on a targeted ad because I feel that my purchases will be monitored.	.716
	Reasons to click	I intend to click on a targeted ad if I need the product, despite my privacy concerns.	.699
		I intend to click on a targeted ad because they are an innovative and creative way of shopping.	.692
		I intend to click on a targeted ad because they cater to my personal interests and needs.	.743
		I intend to click on targeted ads because they improve my online shopping experience.	.694